United States Department of Energy

Technical Qualification Program

Problem Analysis and Risk Assessment Self-Study Guide

Revision 1
October 25, 1996

Albuquerque Operations Office

Table of Contents

List of Figures

List of Tables

Preface

Scope and Background

The scope of this study guide encompasses those competencies identified in the Department of Energy (DOE) Problem Analysis and Risk Assessment Topical Area. The guide seeks to address the skills and knowledge which have been identified in the DOE *General Technical Base Qualification Standard* and other Department-Wide Functional Area Qualification Standards as identified in the training to competancy matrix and the Problem Analysis and Risk Assessment study guide cross-Competency Listing (opposite).

The acquisition of these competencies can be demonstrated by three methods: competency equivalency documented by previous training, education, and experience; competency evaluation of knowledge and skills using examinations and performance evaluations; and competency exemption, which is a written release from the requirement to meet a specific competency. Some general examples of these methods include documentation of equivalent training or education, a test-out (or challenge test), a requirement waiver, completion of applicable course work, and other learning activities (such as this study guide).

Intent

The intent of this study guide is:

- To provide subject matter content in a suitable self-study medium that supports the acquisition of familiar and/or working level skills and knowledge as required by the problem analysis and risk assessment Technical Qualification Program competencies. The scope and content of this study guide, is not meant to support an “expert level” knowledge for the included material.

- To be used as a review for those individuals who have been previously exposed to the material.

How to Use This Study Guide

- For those sections that have a quiz or exercise, use them to gage the level of review needed. Then focus on those sections of the guide for which a review is required.
- Follow the sections in sequence for an overall review of the subject matter.
- For assistance or additional information, don't hesitate to contact your supervisor or subject matter experts at your facility or site, or refer to identified resources as necessary.
- When you have completed the study guide, contact your organizational training administrator for a copy of the exam. The exam is a proctored, closed book exam and the allotted time is one hour. Once you have completed with the exam, present it to the proctor, who will then have the exam evaluated. Results shall be forwarded to you, your supervisor, and your training file.
- Your supervisor (or delegated qualifying official) shall determine whether you have satisfactorily completed the competencies.
- Your Technical Qualification Record will be updated to document the completed competencies.

DISCLAIMER

This guide was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, or any of their contractors, subcontractors, or their employees, makes any warrantee, expressed or implied, or assumes any legal liabilities or responsibility for the accuracy, completeness, or usefulness of information, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency, contractor, or subcontractor thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency, contractor or subcontractor thereof.

Basic Statistics

Section 1

OBJECTIVE

Demonstrate knowledge of solving simple statistics problems, computing simple probabilities, describing probability distributions, and discussing statistical sampling procedures.

Introduction

Introduction - What is Statistics?

To understand problem analysis and risk assessment, it is important to have a solid foundation in the concepts of statistics and probability.

Statistics is a scientific method used to collect, organize, summarize, present, and analyze data. Drawing conclusions and making reasonable decisions on the basis of the data analysis is a second aspect of statistics.

It is far more practical to observe a sample from a group, particularly when the group is large. This translates to sampling a portion of a *population*. If the sample is found to be representative of the population, important conclusions about the population as a whole can be inferred through statistical analysis of the sample. There is however, some *probability* that any sample of a population could be skewed or misrepresentative of the original population. As a result, any discussion of the validity of sample analysis results is spoken of in terms of a *probability* that the data are representative of the original population with some *confidence interval or level*.

1 - 1

1. **State the definition of the following statistical terms and compute its value given sample data.**
   - **mean**
   - **median**
   - **mode**
   - **range**
   - **variance**
   - **standard deviation**

- **mean deviation**
- **coefficient of variance**

A. Measures of Central Tendency

Mean

The *mean*, in general terms, is the average value of the data set. An *average* is a value that is typical or representative of a set of data. The mean of a set of quantitative data is defined as the sum of the measurements divided by the number of measurements contained in the data set.

The *arithmetic mean*, or briefly the mean, of a set of N numbers $X_1, X_2, X_3, \ldots, X_N$ is denoted by $\overline{X}$ (read "X bar"), or the symbol μ for a population, and is defined as

$$\overline{X} = \frac{X_1 + X_2 + X_3 + \cdots + X_N}{N} = \frac{\sum_{j=1}^{N} X_j}{N} = \frac{\sum X}{N}$$

Example:
For the data set 5 3 7 9 8 5 4 5 8, the Mean is:

$$\frac{7+3+5+9+7+5+4+5+9}{9} = \frac{54}{9} = 6$$

Advantages of using Mean $\overline{X}$	Disadvantages of using Mean $\overline{X}$
♦ represents the "center of gravity" of all data ♦ uses all data ♦ requires no sorting	♦ extreme data values or outliers may skew the mean value ♦ may be time consuming to calculate ♦ the mean may not be the actual value of any data set member

Median

The *median* of a set of numbers – arranged in order of magnitude – is either the middle value for a data set with an odd number of members or the average of the two middle values if the data set contains an even number of members.

Example:

	Odd-member set	Even-member set
data set	7 3 5 9 7 5 4 5 9	2 3 6 4 2 7 2 7 9 8
ordered data set	3 4 5 5 **5** 7 7 9 9	2 2 2 3 **4** **6** 7 7 8 9
Median	5	$\frac{4+6}{2}=5$

Advantages of using Median	Disadvantages of using Median
♦ provides an idea of where most data are located ♦ requires little calculation	♦ the data must be sorted and arranged ♦ does not use all the data ♦ does not consider extreme values which may be important

Mode

The *mode* of a set of numbers is that value which occurs with the greatest frequency. The mode may not exist, and even if it does exist, it may not be unique.

Example:

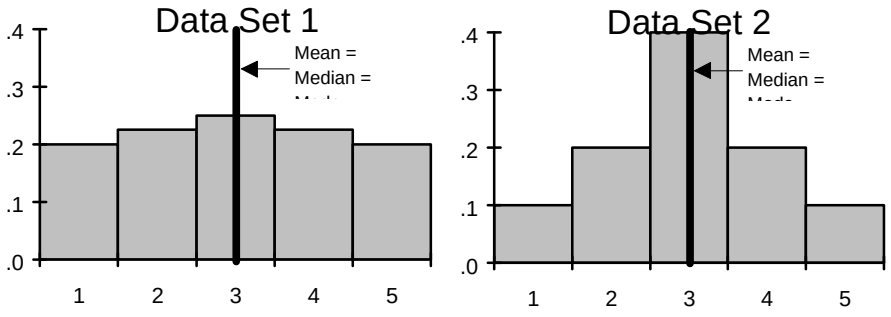
	Example 1	Example 2	Example 3
data set	3 4 **5 5 5** 7 8 8 9	3 5 8 10 12 15 16	2 3 **4 4 4** 5 5 **7 7 7** 9
Mode	5 - unimodal	no mode	4 and 7 - bimodal

Advantages of using Mode	Disadvantages of using Mode
♦ it is not influenced by extreme values ♦ it is an actual value within the data set ♦ it can be detected visually in distribution plots	♦ the data may not have a mode

B. Measures of Variability or Dispersion

In order to have a complete picture of a sample of data, the distribution of the data contained within a given sample must also be measured. Consider the following two data sets that demonstrate this concept.

Figure 1.1



Analyzing and comparing the data in the two histograms displayed in Figure 1.1 reveals that both data sets have the same values for their mean, median, and mode. Note however that data set 1 has a very uniform data measurements spread. Data set 2 on the other hand has most of its measurements clustered about a center value of 3. From these example data sets, it may be seen that data set 2 is *less variable* than data set 1. Stated another way, the data in data set 2 shows a more focused distribution around the mean value of 3 with fewer data points at a distance from the mean when compared to the data in data set 1. From this example, it is evident that a measure describing the variability or distribution of a given data set must accompany any measurement of the mean, median or mode.

Some of the more common measures of variability are variance, standard deviation, and coefficient of variance. These measures will be defined in the following discussions.

Variance

One of the most commonly used measures of data variation is the *variance* which is termed σ^2 for a population and S^2 for a sample. The formulas are

$$\text{Population or } s^2 = \frac{\sum (X - m)^2}{N} \qquad \text{Sample or } S^2 = \frac{\sum (X - \bar{X})^2}{N - 1}$$

Example:
This example shows how to calculate a sample variance.

Step 1. Compute the sample mean.

Step 2. Compute the deviation of each measurement from the mean: $(X - \overline{X})$

Step 3. Square each deviation: $(X - \overline{X})^2$

Step 4. Sum the square deviations: $\sum(X - \overline{X})^2$

Step 5. Divide the sum by (number of measurements – 1).

sample measurements	1	2	3	4	5
mean or $\overline{X}$	$\frac{1+2+3+4+5}{5} = \frac{15}{3} = 3$				
$X - \overline{X}$	1 - 3 -2	2 - 3 -1	3 - 3 0	4 - 3 1	5 - 3 2
$(X - \overline{X})^2$	4	1	0	1	4
$\sum(X - \overline{X})^2$	4 + 1 + 0 + 1 + 4 = 10				
$S^2 = \frac{\sum(X - \overline{X})^2}{N-1}$	$\frac{10}{5-1} = \frac{10}{4} = 2.5$				

Standard Deviation

The *standard deviation* is the square root of variance. The formulas for standard deviation are:

Population or $s = \sqrt{\frac{\sum(X-m)^2}{N}}$ Sample or $S = \sqrt{\frac{\sum(X-\overline{X})^2}{N-1}}$

Example:
The standard deviation for the above example would be:

$$S = \sqrt{S^2} = \sqrt{\frac{\sum(X-\overline{X})^2}{N-1}} = \sqrt{2.5} = 158$$

Coefficient of Variance

The measurement of the variation, or dispersion using the standard deviation is commonly referred to as the *absolute dispersion*. Depending on the value being measured, the relative deviation from the measured value may be quite different. For example, a variation (or dispersion) of 5°F in measuring a temperature range of 210°F is quite different, in effect, from the same variation of 5°F in a temperature range of 20°F. This forms the basis for a measurement of the *relative dispersion*, which is defined by $\frac{\text{absolute dispersion}}{\text{average}}$.

Example:
If the absolute dispersion associated with a sample is found to be *S* with a mean of $\overline{X}$, then the relative dispersion or the *coefficient of variance/dispersion* is defined by $V = \frac{S}{\overline{X}} \times 100$. For an entire population measurement, it is defined by $V = \frac{s}{m} \times 100$. *Coefficient of variance or dispersion* is usually expressed as a percentage.

Continuing the example using the sample measurements 1, 2, 3, 4 and 5, the coefficient of variance would be calculated as

$$\frac{S = 158}{\overline{X} = 3} = .526 \times 100 = 52.6\%.$$

2. Define Probability and calculate simple probabilities of events given sample data.

1 - 2

Probability

Probability is the likelihood of the occurrence of an event.

Simple Events

A *simple event* is the most basic outcome of an experiment, and an *experiment* is the process of making an observation or taking a measurement. The collection of all simple events from an experiment is defined as a *sample space*. The probability of a simple event *A* is calculated by summing the occurrences of the simple event *A* and dividing by the sample space or the total number of simple events observed. The probabilities assigned to a simple event must obey two rules:

1. all simple event probabilities must lie between 0 and 1
2. the probabilities of all simple events within a sample space must sum to 1.

Example:
Consider a simple experiment of tossing a die and observing the number on the up face. The six possible outcomes to the experiment are:

1. observe a 1
2. observe a 2
3. observe a 3
4. observe a 4
5. observe a 5
6. observe a 6.

Since these six possible outcomes cannot be decomposed into more basic outcomes, they are the simple events of this experiment. This is the sample space for the experiment, and it can be represented in set notation as a set of six simple events: *S:* {1, 2, 3, 4, 5, 6}. If an experiment is repeated a large number of times (*N*) and the event (*E*) is observed n_E times, the probability of *E* is approximately $P_E = \frac{n_E}{N}$.

Example:
The probability of observing 3 on the toss of a single die is $P_3 = 1 \div 6 = .166$.

Compound Events

Compound events are formed by either the union or the intersection of two or more events. For the following we define: E_A = A and E_B = B.

The union of A and B is denoted by $A \cup B$. If A and B are two events in a sample space S, then $A \cup B$ contains all sample points in **either** event A, event B, or both.

Example:
Consider again the toss of a die.
A = E_1, E_2, (values less than 3)
B = E_1, E_3, E_5 (odd values)
$A \cup B$ = E_1, E_2, E_3, E_5
The probability of rolling either a value less than 3 or an odd value is:
$P(E_{T)}) = P(E_1) + P(E_2) + P(E_3) + P(E_5) = 1/6 + 1/6 + 1/6 + 1/6 = 4/6 = 2/3 = .666$

The intersection of A and B is denoted by $A \cap B$ or AB. If A and B are two events in a sample space S, $A \cap B$ is composed only of all those sample points that are contained in **both** A and B.

Example:
Consider the same sets A and B in the above example.

$A \cap B = E_1$

The probability of rolling an odd value less than three is

$PE_{A \cap B} = P(E_1) = 1/6 = .167$

Conditional Probability

The event probabilities calculated so far have been *unconditional probabilities* since no special conditions are assumed. If additional information which would alter the outcome of an event is available, this would change the probability of an event occurrence. This probability is termed *conditional probability*. For example, the probability of drawing an ace from a deck of 52 cards is .077 (4/52). However, suppose you had already drawn a card from the deck, a 7 of diamonds (event B). Is the probability of drawing an ace still .077? Since event B has already occurred, the sample space is reduced from 52 simple events to 51 simple events. Since the are only 51 simple events in the reduced sample space, the probability that A occurs *given that B occurred* is 4 in 51 or .078. To find the conditional probability that event A occurs *given that event B occurs*, divide the probability that both A and B occur by the probability that B occurs.

The conditional probability of event A given that B has occurred is denoted by $P(A|B) = \frac{P(A \cap B)}{P(B)}$ if $P(B) \neq 0$. Using this notation for our example $P(A|B) = \frac{P(\text{Seven}) \times P(\text{Ace})}{P(4\ )} = \frac{\frac{4}{52} x \frac{4}{51}}{\frac{4}{52}} = \frac{4}{51}$

Note that since unions and intersections of events are events also, we can always calculate their probabilities by adding the simple event probabilities of which they are composed.

Before moving on to discuss the additive and multiplicative laws, two other terms just mentioned must be defined: independent and mutually exclusive.

Events A and B are *independent* if the occurrence of B does not alter the probability that A has occurred, or P(A|B) = P(A). If events A and B are independent, it is also true that P(B|A) = P(B). If events A and B are not independent they must be *dependent*.

Events A and B are *mutually exclusive* if $A \cap B$ contains no simple events. If two events A and B are mutually exclusive, the probability of the union of A and B equals the sum of the probabilities of A and B or $P(A \cup B) = P(A) + P(B)$. These concepts are explained further in the following sections.

Additive Law

If two events are not mutually exclusive, the probability of the union of events A and B does not equal the sum of the probability of event A and event B. This results in the additive law and it is denoted by $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

Example:

Toss a single die and observe the up face. The following events and probabilities are defined:

A: {observe an odd value less than 4} P(A) = P(1) + P(3) = .333

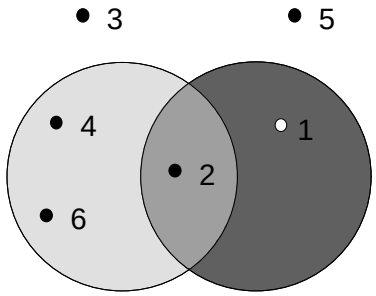
B: {observe a value < 3} P(B) = P(1) + P(2) = .333

$P(A \cap B) = P(1) = .167$

A Venn diagram, as shown in the following page, is helpful in showing that $P(A \cup B)$ equals P(1) + P(2) + P(3). It also shows that $P(A \cap B) = P(1)$. If P(A) and P(B) are added together the sum becomes: P(A) + P(B) = P(1) + P(3) + P(1) + P(2). The term P(1) appears in the sum twice, and also happens to be $P(A \cap B)$. If the formula $P(A \cup B) = P(A) + P(B) - P(A \cap B)$ is applied, the probability of the union or $P(A \cup B)$ becomes .333 + .333 - .167 = .499.

Figure 1.2

Venn Diagram for Die Toss



Example:
You own two cement mixers and the probability of each mixer starting on a cold morning is .9. What is the probability of getting at least one of them started to go to mix cement?

$P(A \cup B) = P(A) + P(B) - P(A \cap B)$
$= .9 + .9 - (.9 \times .9)$
$= 1.8 - .81$
$= .99$ or 99%

If however, the events are mutually exclusive, the additive law reduces to $P(A \cup B) = P(A) + P(B)$.

Example
What is the probability of drawing an ace or the queen of hearts from a deck of ordinary cards?

$$P(A \cup B) = P(\text{Ace}) + P(\text{Q of hearts}) = \frac{4}{52} + \frac{1}{52} = \frac{5}{52} = .096$$

Note that the key word in the additive law is OR. Also, you may tell if events are mutually exclusive by asking the do the desired events share any common sample points? In out above three examples, the following are observed:

- For the dice example, there is a possible intersection in rolling a 2.
- For the cement mixer example, there is a possible intersection in that both of them may start.
- For the deck of cards example, there is no possible intersection in that no card could be drawn that contains both an ace and the queen of hearts.

1 - 3 Multiplicative Law

The multiplicative rule of probability can be used to find the probability of the intersection of two events. If the two events are dependent, it was previously determined that $P(A|B) = \frac{P(A \cap B)}{P(B)}$. Multiplying by P(B) gives P(A|B) x P(B) = P(A∩ B) = P(AB). This may be demonstrated by the following (dependent) example.

Example:
What is the probability of drawing an ace of hearts from a deck of ordinary cards in two successive draws?

$$P(A \cap B) = P(Ace) + P(Ace|Ace) = \frac{4}{52} x \frac{3}{51} = \frac{12}{2652} = .005$$

If the two events are independent, the multiplicative law is simply a product of the two independent probabilities, or P(AB) = P(A) x P(B). This is demonstrated by the following independent example.

Example:
A farmer is interested in plowing his field on a day when it is not raining in the spring, therefore he is concerned with the following two events:

A: {the operation of his tractor in the spring}

B: {a dry day in the spring}

Based on available information, the farmer believes that the probability is .9 that the tractor will work and that the probability of rain is .1 *during* the spring season on any day.

P(A) = .9

P(B|A) = .9

Note that P(B|A) is calculated by taking 1- (the probability of rain = .1) =.9.

Based on the information provided, what is the probability that the farmer will plow his field on a dry day in the spring. In other words, what is the intersection of events A and B or P(A∩ B)?

To quantify the example, we note that the two events are independent and therefore the intersection of events A and B is (.9)(.9) = .81. This gives the probability that the farmer will plow his field and it will not rain while he is plowing (in the spring) as .81.

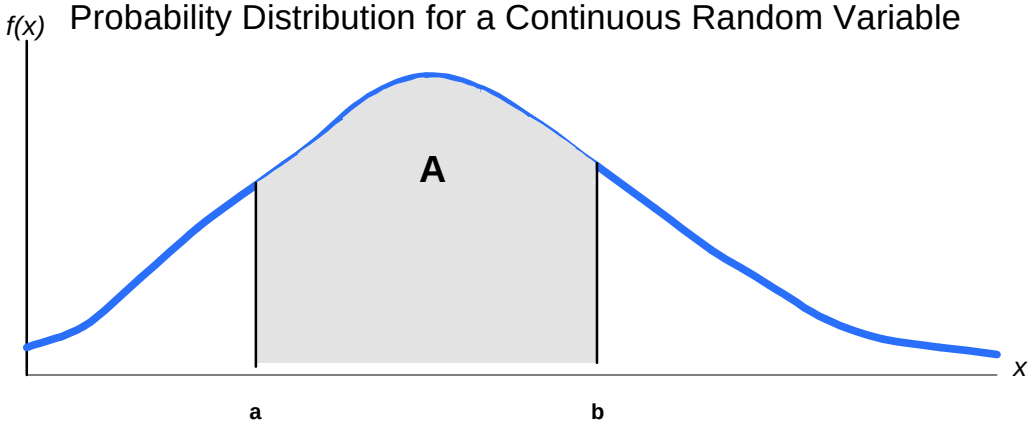
3. Describe and explain the structure of a normal distribution and a log normal distribution.

Probability Distribution

If a variable *x* can only assume a discrete set of values x_1, x_2, …, x_K with corresponding probabilities of p_1, p_2, …, p_K, where the sum of p_1, p_2, …p_K = 1, a discrete probability distribution for *x* called the *probability function* or *frequency function* of *x* has been defined. Because *x* can only assume specific values with associated probabilities, it is often called a *discrete random variable*. This is opposed to x values that can assume any value contained in one or more intervals and for which the associated probability function is *continuous*.

The *probability distribution* for a discrete random variable is a graph, table, or formula that correlates the probability associated to each possible value the discrete random variable can assume. The form of the probability distribution for a *continuous random variable* is a smooth curve that might appear as shown in Figure 1.3. The areas under a probability distribution correspond to probabilities for *x*. For example, the area *A* beneath the curve between the two points *a* and *b*, as shown in Figure 1.3, is the probability that *x* assumes a value between *a* and *b* ($a < x < b$). Because there is no area over a point, say $x = a$, it follows that the probability associated with a particular value of *x* is equal to zero; or $P(x = a) = 0$. Also, because areas over intervals represent probabilities, the total area under the probability distribution is equal to 1.

Figure 1.3 Probability Distribution for a Continuous Random Variable



Example:
Let a pair of standard dice be rolled and let *x* represent the sum of the values for the two dice rolled for each roll. The resulting

probability distribution is given in Table 1.1. As an example, the probability of getting a sum of 7 is 6/36 = 1/6. Following 300 rolls of the two dice, we would expect to see 50 of them give a combined sum of 7.

Figure

Table 1.1

x	2	3	4	5	6	7	8	9	10	11	12
$p(x)$	1/36	2/36	3/36	4/36	5/36	6/36	5/36	4/36	3/36	2/36	1/36

Table 1.1

The Normal Distribution

The bell curve is one of the most commonly observed continuous random variable probability distributions. Its probability distribution is a normal distribution. The normal distribution is symmetric about its mean value, μ, and it has a spread that is determined by σ, its standard deviation. The formula for the normal probability distribution is given by:

$$f(x) = \frac{1}{s\sqrt{2p}} e^{-(1/2)[(x-m)/s]^2},$$

where

μ = Mean of the normal random variable x

σ = Standard deviation

π = 3.1416…

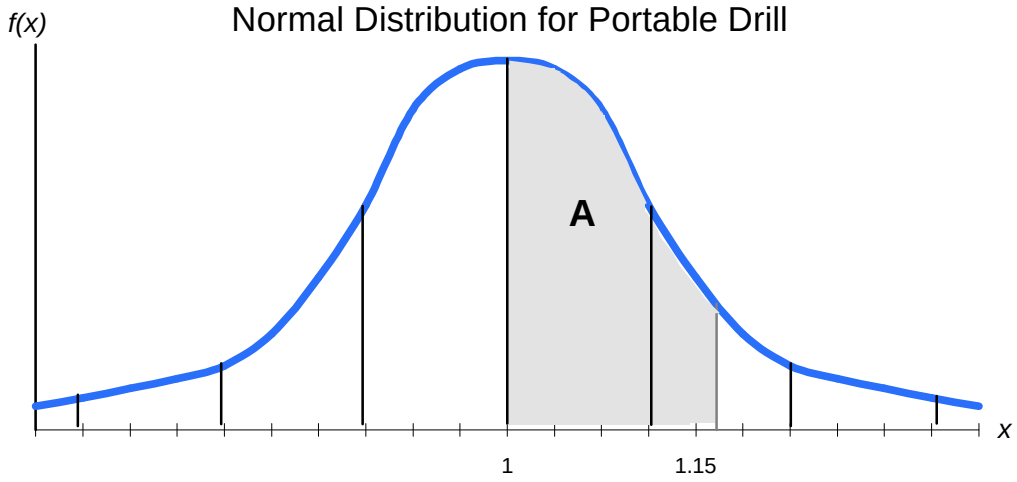
e = 2.71828…

Z-Score

To simplify working with normal curves areas under the normal curve are usually listed in a table. However, since there is a different curve for each pair of values for μ and σ, a single table of areas as a function of *z-score* is defined for use with any normal curve. The formula for the z-score is denoted as $z = \frac{x-m}{s}$. Note that when $x = m$, z becomes 0.

Example:

Suppose we know that the during continuous usage, the length of time between charges for a portable drill is defined by a normal distribution with a mean of 1 hour and a standard deviation of 6 minutes or 0.1 hours. If we observe the length of between successive charges, what is the probability the time observed will be between 1 and 1.15 hours. This probability is shown as the shaded shaded area *A* of Figure 1.4.



The first step in determining the probability designated by the shaded area *A* is to calculate the z-score corresponding to the measurement 1.15:

$$z = \frac{x - m}{s} = \frac{1.15 - 1}{0.1} = 1.5$$

The next step is to refer to a normal curve area *"z"* table part of which is found as Table 1.2. Note that the z-scores are listed in the left-hand column of the table. To find the area corresponding to a z-score of 1.5, first locate the value 1.5 in the left-hand column. Since this column lists *z* values to one decimal place only, if the value had been out to two decimal places, we would also refer to the top row of the table. Last, locate the number under the vertical column where the*z* = 1.5. This number represents the shaded area A and has a value of .4332.

Consequently, the probability that the drill operates between 1 and 1.1 hours before needing a charge is .4332.

Table 1.2

Normal Curve Areas

z	**.00**	.01	.02	.03	.04	.05	.06	.07	.08	.09
1.1	.3643	.3665	.3686	.3708	.3729	.3749	.3770	.3790	.3810	.3830
1.2	.3849	.3869	.3888	.3907	.3925	.3944	.3962	.3980	.3997	.4015
1.3	.4032	.4049	.4066	.4082	.4099	.4115	.4131	.4147	.4162	.4177
1.4	.4192	.4207	.4222	.4236	.4251	.4265	.4279	.4292	.4306	.4319
1.5	**.4332**	.4345	.4357	.4370	.4382	.4394	.4406	.4418	.4429	.4441

Log-Normal Distribution

In probabilistic risk assessment, normal distributions are frequently used to describe equipment which has increasing failure rates with time. A log-normal distribution is similar to a normal distribution with the exception that the logarithms of the values of the random variables, rather than the values themselves, are assumed to be normally distributed. Thus, all values are positive, the distribution is skewed to the right, and the skew is a function of an error factor. Log-normal distributions are encountered frequently in metal fatigue testing, maintainability data (time to repair), and chemical process equipment failures and repairs.

1 - 4

4. Discuss the terms confidence interval and confidence limit. Calculate a confidence interval given the appropriate data.

A discussion on confidence intervals and limits for a probability distribution must begin with an overview of the properties of the sampling distribution and calculation of the sampling distribution's mean and standard deviation ($\bar{x}$ and s).

Estimating the mean useful life of batteries, the mean number of traffic accidents per month for a high traffic density intersection, and the mean number of hamburgers used per month at a restaurant are practical problems where one is interested in making an inference about the mean μ of some population. The sample mean, $\bar{x}$ is generally a good estimator of μ.

The sampling distribution of $\bar{x}$ has the following three properties.

1. the mean of the sampling distribution = the mean of sampled population. That is $m_{\bar{x}} = m$.
2. the standard deviation of the sampling distribution =

$\frac{\text{the standard deviation of the sampled population}}{\sqrt{\text{sample size}}}$. That is $s_{\bar{x}} = \frac{s}{\sqrt{n}}$.

3. The sampling distribution of $\bar{x}$ is approximately normal for large sample sizes.

The justification for property 3 is contained in one of the most important statistical theories, the *central limit theorem* which states:

> For large sample sizes, the mean $\bar{x}$ of a sample from a population with mean μ and standard deviation σ possesses a sampling distribution that is approximately normal *regardless of the probability distribution of the sampled population*. The larger the sample size, the better will be the normal approximation to the sampling distribution of $\bar{x}$.

Example:
Suppose a large hotel chain wants to estimate the average length of time customers stay at their hotel. To accomplish this objective, hotel management plans to sample 200 of all previous customer records and use the sample mean of the lengths of stay to estimate the mean stay length of *all* customers. Further, they plan to use the sampling distribution of the sample mean to assess the accuracy of their estimate. From the central limit theorem, the sampling distribution of the sample mean is approximately normal for large samples.

Assume the interval of interest is given by $\bar{x} \pm 2s_{\bar{x}} = \bar{x} \pm \frac{2s}{\sqrt{n}}$, corresponding to an interval with endpoints located 2 standard deviations on either side of the sample mean. Determine what are the chances that this interval will enclose the population mean, μ?

A graphical representation of this question is given in Figure 1.5. From this figure, it is evident that if the 200 measurements yield a value of $\bar{x}$ that falls between the interval shown in gray (2 standard deviations of μ), then the interval $\bar{x} \pm 2s_{\bar{x}}$ will contain μ. If $\bar{x}$ falls outside these boundaries, the interval $\bar{x} \pm 2s_{\bar{x}}$ will not contain μ. Since the area under the normal curve (the sampling distribution of $\bar{x}$) between these boundaries is about .95 (or precisely .9544) we know that the interval $\bar{x} \pm 2s_{\bar{x}}$ will contain μ with a probability approximately equal to .95.

Sampling Distribution of $\bar{x}$

Example:
Suppose that the sum and the sum of squared deviations for the sample of 200 lengths of time spent in the hotel are $\sum x = 770$ days and $\sum (x - \bar{x})^2 = 2{,}907$ respectively. Then

$\bar{x} = \frac{\sum x}{n} = \frac{770}{200} = 3.85$ and $s^2 = \frac{\sum (x - \bar{x})^2}{n - 1} = \frac{2907}{199} = 14.61$ and s = 3.8.

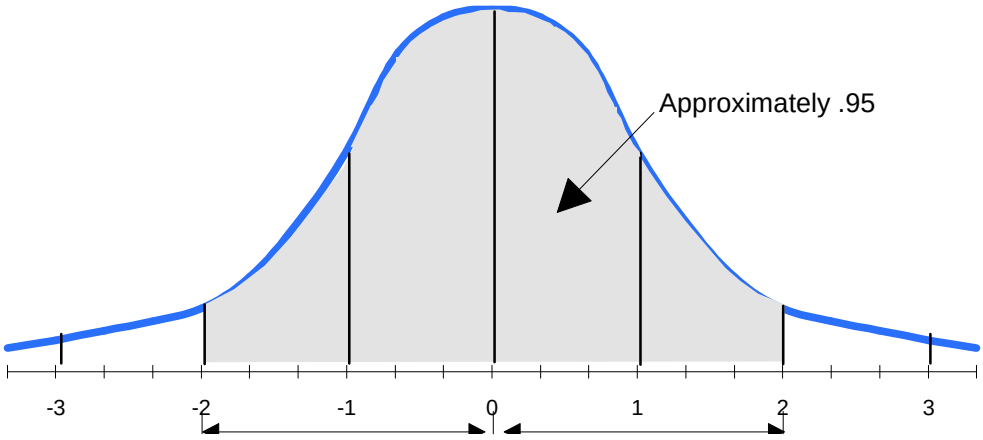


Figure 1.5

To form the interval two standard deviations around $\bar{x}$, calculate

$\bar{x} \pm 2s_{\bar{x}} = 3.85 \pm 2\frac{s}{\sqrt{200}}$.

From this it is evident that without knowing the standard deviation of the original population, (the standard deviation of the lengths of stay for *all* patients), the interval cannot be calculated. However, since the sample is large (n = 200 measurements), the interval may be approximated by using the sample standard deviation s as an estimate of σ. This results in

$\bar{x} \pm 2\frac{s}{\sqrt{200}} \approx \bar{x} \pm 2\frac{s}{\sqrt{200}} = 3.85 \pm 2\left(\frac{3.8}{14.14}\right) = 3.85 \pm .54$. As a result, the mean length of stay in the hotel for all guests is estimated to fall in the interval of 3.31 to 4.39 days.

Confidence Interval

Is μ, the true mean, in the interval 3.31 to 4.39 days? This issue cannot be stated with certainty, but by determining a confidence interval a statistical estimate may be made as to with what certainty it is. This confidence is derived from the knowledge that if numerous random samples of 200 measurements from this population were drawn and an interval of 2 standard deviations was formed around $\bar{x}$ each time, approximately 95% of the intervals would contain μ.

There is no way of knowing whether any given sample is one of the 95% that contain μ. As a result, the interval of 3.31 to 4.39 days provides an estimate of the mean length of time that customer stays at the hotel. The formula that tells us how to calculate an interval estimate based on sample data is called an *interval estimator*. The probability, .95, that measures the confidence we can place in the interval estimate is called a *confidence coefficient*. The percentage, 95% in this case, is called the *confidence level* for the interval estimate.

If a confidence coefficient other than .95 is chosen, the total area under the sampling distribution would increase from that which was previously shown in **Figure 1.5**, with the remainder being equally divided between the two tails. If a confidence interval is chosen and the remainder is to be split between the tails (let it be designated α) as shown in Figure 1.6, this is the standard normal curve for locating $z_{\alpha/2}$. For example, if an area of $\alpha/2$ is placed in each tail and if $z_{\alpha/2}$ is designated as the z-value such that the area $\alpha/2$ will still lie to its right, then the confidence interval with confidence coefficient $(1 - \alpha)$ is found to be $\bar{x} = z_{a/2} s_{\bar{x}}$.

To illustrate this for a confidence coefficient of .90,$(1 - \alpha) = .90$, $\alpha = .10$, $\alpha/2 = .05$, and $z_{.05}$ is the z-value that correlates to an area of .05 in the upper and lower tail of the sampling distribution. Recall that a table is used to determine the area between the mean and a specified z-value. Since the total area to the right of the mean must be .5, $z_{.05}$ will correspond to the z-value of an area calculated to be .5 - .05 = .45. This is depicted graphically in Figure 1.6. The z-value corresponding to an area of .45 is $z_{05} = 1.645$. For most cases of interest, confidence coefficients used in practice will range from .90 to .99. The most common confidence coefficients with corresponding values of α and $z_{\alpha/2}$ are given in Table 1.3.

The z-Value Corresponding to an Area Equal to .05
in the Upper Tail of a z-Distribution

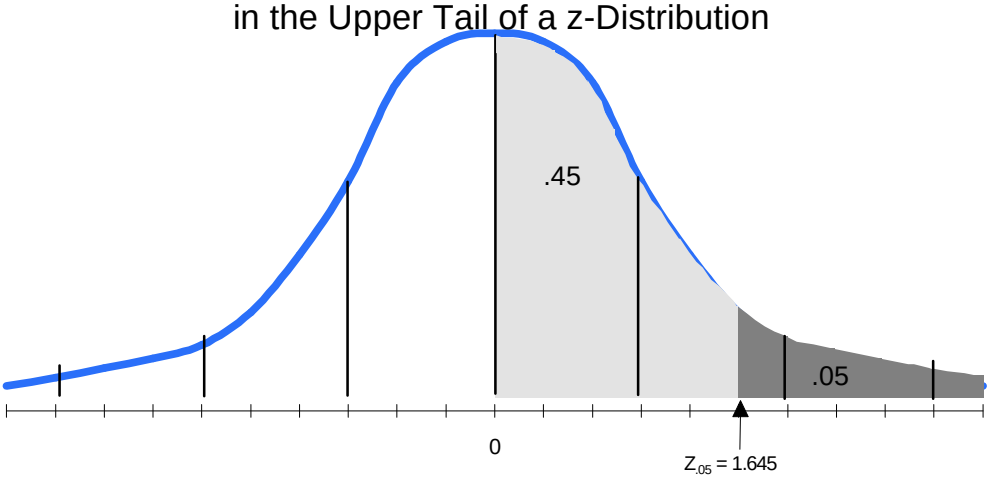


Figure 1.6

Commonly Used Values of $z_{\alpha/2}$

Table 1.3

Confidence Level 100 (1 - α)	α	α/2	$z_{\alpha/2}$
90%	.10	.050	1.645
95%	.05	.025	1.960
99%	.01	.005	2.580

Sample problem:
Suppose a theater wants to estimate its average number of unoccupied seats during the afternoon matinee G rated movie over the past year. To accomplish this, the attendance records for 40 different movies shown as matinees are randomly selected from the files, and the number of unoccupied seats (as measured by unsold tickets) is noted for each. The sample mean $\bar{x} = 32.6$ seats and the standard deviation s = 7.3 seats. Compute μ, the mean number of unoccupied seats per G rated matinee movie over the past year using a 90% confidence interval and provide the interval.

Solution:
The general form of the 90% confidence interval for a population mean is $\bar{x} \pm z_{a/2} s_{\bar{x}} = \bar{x} \pm z_{.05} s_{\bar{x}} = \bar{x} \pm 1645\left(\frac{s}{\sqrt{n}}\right)$. For the 40 records sampled, we have $32.6 \pm 1.645\left(\frac{s}{\sqrt{40}}\right)$. Again, σ is not known so the sample standard deviation s will be used to estimate σ. Using s, the

90% confidence interval is approximately,

$32.6 \pm 1.645\left(\frac{7.3}{\sqrt{40}}\right) = 32.6 \pm 1.9$ or from 30.7 to 34.5. This gives, at a 90% confidence level the mean number of per G rated unoccupied matinee movie seats per movie during the sampled year. To reiterate, if this procedure were applied repeatedly to different samples, approximately 90% of the sample intervals would contain μ.

1 - 5

5. Describe the following sampling procedures and provide an example of each one.

- **acceptance**
- **variable**
- **random**
- **stratified**
- **cluster sampling**

Sampling Overview

Sampling is the process of evaluating of a portion of a population by using a lot, batch, or other type of statistical sampling process. From the sample, useful information is determined about the parent population as a whole. As an example, by inspection of a sample specific information concerning quality attributes, color variation, length variance, thickness, etc., of the pieces in a lot may be examined to better understand these same attributes as they represent a statistical sample of the parent population. This process also provides knowledge about the process which produced the lot from which the sample was taken. Using the sample information, it is possible to draw conclusions as to whether the production process and the associated product meet some minimum statistical standard, that is, is the lot good or bad. This knowledge may then be used to make assumptions about the quality of uninspected pieces.

The primary advantage of sampling a statistically representative lot over 100 percent inspection is the reduction in production costs while maintaining an expected level of quality. In addition, sampling offers additional advantages such as:

- provides a process control adequacy check
- reduces the amount of handling and therefore damage caused by inspection

- improves the delivery schedule since only a portion of the product is sampled
- rejection on entire lots provides stronger motivation for improvement by suppliers
- inspection is to lot-by-lot decisions versus piece by piece.

The process of sampling also has disadvantages including:

- a small risk of rejecting “good” products and accepting an entire lot of a “bad” product
- additional costs and administrative burden for planning and documentation
- only statistical product information availability when compared to 100 percent inspection.

Acceptance sampling must distinguish whether the purpose is to accumulate information on the immediate *product* being sampled or on the *process* which produced that same lot. This results in two types of sampling:

Type A - Sampling of the lot of product on hand for acceptance or rejection.

Type B - Sampling of the lot of product on hand to determine if the process which produced the lot was is within acceptable limits.

Two other factors enter into the analysis of a sample:

- the type of sampling determines the appropriate probability distribution for use in characterization of plan performance, and
- the type of data generated.

Several types of sampling and illustrative examples will be provided in this section, including: acceptance, variable, random, stratified, and cluster.

Acceptance Sampling

Acceptance sampling is concerned with two types of data. *Attribute* data can be characterized as go/no-go information. It involves the measurement of defectives and defects. *Defectives* refers to the acceptability of units of product for a wide range of characteristics. It is usually measured in proportion or percent defective. *Defects* are the number of defects found in the units inspected, and it is possible for the number of defects to exceed the number of units inspected.

Defects are measured by actual account or as a ratio of defects per unit. *Variables* provide measurement information, and they refer to the distribution of a specific measurable characteristic of the inspected product. Variables are usually measured by the mean and standard deviation.

Acceptance Sampling Plans

Since acceptance sampling contains two different types of data, two different sampling plans can be created. All attribute sampling plans are based on data that can be counted. In attribute plans, a sample is taken from a lot with each unit classified as acceptable or defective. The number of defects is then compared to a specified acceptance number, in order to make an accept or reject decision for the lot. Examples of acceptance plans are MIL-STD-105E, ANSI/ASQC Z1.4, and Dodge-Romig Tables.

Attribute Sampling Plan Example – MIL-STD-105E

MIL-STD-105E is based on a high probability of acceptance (85-99%). The standard consists of tables listing sample size code letters and tables that delineate acceptance and rejection numbers. A total of two numbers are necessary to enter a single sampling plan into MIL-STD-105E. Based upon these two sample variables, the maximum number of defectives is defined for the lot to still be acceptable. The three variables that must be entered are: N = lot size, n = sample size, and an inspection level. Using these the Ac = c = the maximum number of defectives is defined for the lot.

The following is a simple example using a MIL-STD-105E code letter index and a single sampling table for normal inspection. In this example, a lot size of 600 pieces, an AQL (acceptable quality level) of 4%, and general inspection level II are specified. By inspecting the MIL-STD-105E Code Letters for Sample Size table, you will see that the sample code is J for the above described lot.

Table 1.4 MIL-STD-105E Code Letters for Sample Size Table

	Special Inspection Levels	General Levels

Lot Size			S-1	S-2	S-3	S-4	I	**II**	III
2	to	8	A	A	A	A	A	A	B
9	to	15	A	A	A	A	A	B	C
16	to	25	A	A	B	B	B	C	D
26	to	50	A	B	B	C	C	D	E
51	to	90	B	B	C	C	C	E	F
91	to	150	B	B	C	D	D	F	G
151	to	280	B	C	D	E	E	G	H
281	to	500	B	C	D	E	F	H	J
501	**to**	**1200**	C	C	E	F	G	**J**	K
1201	to	3200	C	D	E	G	H	K	L
3201	to	10000	C	D	F	G	J	L	M
10001	to	35000	C	D	F	H	K	M	N
35001	to	15000	D	E	G	J	L	N	P
150001	to	500000	D	E	G	J	M	P	Q
	>	500001	D	E	H	K	N	Q	R

In the Single Sampling Table, we look at the column for AQL = 4.0. Next we look for the intersection of this column with the row for Sample Size Code Letter = J. The acceptance number = 7, the rejection number = 8, and the sample size = 80. The reader is referred to the actual standard for a complete discussion of special inspection and general levels.

Table 1.5

MIL-STD-105 Single Sampling Tables Normal Inspection

Sample Size Code Letter	Acceptable Quality Levels																						Sample Size
	.040		.065		1.0		1.5		2.5		**4.0**		6.5		10		15		25		40		
	Ac	Re	Ac	Re	Ac	Re	Ac	Re	Ac	Re	Ac	Re	Ac	Re	Ac	Re	Ac	Re	Ac	Re	Ac	Re	
A	⇩		⇩		⇩		⇩		⇩		↓		0	1	⇩		↓		1	2	2	3	2
B	⇩		⇩		⇩		⇩		↓		0	1	↑		↓		1	2	2	3	3	4	3
C	⇩		⇩		⇩		↓		0	1	↑		↓		1	2	2	3	3	4	5	6	5
D	⇩		⇩		↓		0	1	↑		↓		1	2	2	3	3	4	5	6	7	8	8
E	⇩		↓		0	1	↑		↓		1	2	2	3	3	4	5	6	7	8	10	11	13
F	↓		0	1	↑		↓		1	2	2	3	3	4	5	6	7	8	10	11	14	15	20
G	0	1	↑		↓		1	2	2	3	3	4	5	6	7	8	10	11	14	15	21	22	32
H	↑		↓		1	2	2	3	3	4	5	6	7	8	10	11	14	15	21	22	↑		50
J	↓		1	2	2	3	3	4	5	6	**7**	**8**	10	11	14	15	21	22	↑		⇩		**80**
K	1	2	2	3	3	4	5	6	7	8	10	11	14	15	21	22	↑		⇩		⇩		125
L	2	3	3	4	5	6	7	8	10	11	14	15	21	22	↑		⇩		⇩		⇩		200
M	3	4	5	6	7	8	10	11	14	15	21	22	↑		⇩		⇩		⇩		⇩		315
N	5	6	7	8	10	11	14	15	21	22	↑		⇩		⇩		⇩		⇩		⇩		500
P	7	8	10	11	14	15	21	22	↑		⇩		⇩		⇩		⇩		⇩		⇩		800
Q	10	11	14	15	21	22	↑		⇩		⇩		⇩		⇩		⇩		⇩		⇩		1250
R	14	15	21	22	↑		⇩		⇩		⇩		⇩		⇩		⇩		⇩		⇩		2000

⇩ Use the first sampling plan and size below the arrow. If the sample size equals or exceeds the lot size, inspect the whole lot.

↑ Use the first sampling plan and sample size above the arrow.

Ac The acceptance number. If the number of defectives is equal to or less than this number, remove the defectives and accept the balance of the lot.

Re The rejection number. If the number of defectives is equal to or greater than this number, reject the whole lot.

Variable Sampling Plans

In variable sampling plans, a sample is taken and one or more quality characteristic measurements are made on each unit. From these measurements, the sample average or standard deviation is developed to be compared against a critical value defined in the plan. Based upon the comparison, a decision is made to accept or reject the lot. Examples of variable sampling plans are MIL-STD-414 and ANSI/ASQC Z1.9.

Variable Sampling Plan Example – MIL-STD-414

MIL-STD-414 has four sections:

Section A: Introduction

Section B: Sampling plans that are used when the variability is unknown, and the standard deviation method is used.

Section C: Sampling plans that are used when the variability is unknown, and the range method is used.

Section D: Sampling plans that are used when the variability is known.

There are five inspection levels contained in MIL-STD-414. These are levels I, II, III, IV, and V. Generally, if no level has been specified, use level IV.

The following must be specified to use MIL-STD-414:

- the inspection level
- the method (either standard deviation or range)
- the AQL
- the lot size.

As in the previous MIL-STD, the lot size is used to determine sample size code letter. (Note: The grayed cells in the following table are referred to by the example which follows the tables.)

Sample-Size Code Letters

Table 1.6

Lot Size	Inspection Levels				
	I	II	III	**IV**	V
3-8	B	B	B	B	C
9-15	B	B	B	B	D
16-25	B	B	B	C	E
26-40	B	B	B	D	F
41-65	B	B	C	E	G
66-110	B	B	D	**F**	H
111-180	B	C	E	G	I
181-300	B	D	F	H	J
301-500	C	E	G	I	K
501-800	D	F	H	J	L
801-1,300	E	G	I	K	L
1,301-3,200	F	H	J	L	M
3,201-8,000	G	I	L	M	N
8,001-2,2000	H	J	M	N	O
22,001-110,000	I	K	N	O	P
110,001-550,000	I	K	O	P	Q

550,001 and over	I	K	P	Q	Q

An AQL conversion chart is required to align the standard AQL's used in all MIL-STD-414 tables. The AQL's range is from 0.04 to 15.0.

Table 1.7

AQL Conversion Table

For specified AQL values falling within these ranges	Use this AQL value
_____ to 0.049	0.04
0.050 to 0.069	0.065
0.070 to 0.109	0.10
0.110 to 0.164	0.15
0.165 to 0.279	0.25
0.280 to 0.439	.040
0.440 to 0.699	.065
0.700 to 1.090	**1.0**
1.10 to 1.64	1.5
1.65 to 2.79	2.5
2.80 to 4.39	4.0
4.40 to 6.99	6.5
7.00 to 10.9	10.0
11.00 to 16.40	15.0

Table 1.8

Master Table for Normal and Tightened Inspection

Sample size code letter	Sample Size	Acceptable quality levels (normal inspection)										
		0.10 k	0.15 k	0.25 k	0.40 k	0.65 k	**1.00** k	1.50 k	2.50 k	4.00 k	6.50 k	10.0 k
B	3	⇗	⇗	⇗	⇗	⇗	↓	↓	1.12	.958	.765	.566
C	4	⇗	⇗	⇗	⇗	↓	1.45	1.34	1.17	1.01	.814	.617
D	5	⇗	⇗	↓	↓	1.65	1.53	1.40	1.24	1.07	.874	.675
E	7	⇗	↓	2.00	1.88	1.75	1.62	1.50	1.33	1.15	.955	.755
F	**10**	↓	2.24	2.11	1.98	1.84	1.72	1.58	1.41	1.23	1.03	.828
G	15	2.42	2.32	2.20	2.06	1.91	1.79	1.65	1.47	1.30	1.09	.886
H	20	2.47	2.36	2.24	2.11	1.96	1.82	1.69	1.51	1.33	1.12	.917
I	25	2.50	2.40	2.26	2.14	1.98	1.85	1.72	1.53	1.35	1.14	.936
J	30	2.51	2.41	2.28	2.15	2.00	1.86	1.73	1.55	1.36	1.15	.946
K	35	2.54	2.45	2.31	2.18	2.03	1.89	1.76	1.57	1.39	1.18	.969
L	40	2.55	2.11	2.31	2.18	2.03	1.89	1.76	1.58	1.39	1.18	.971
M	50	2.60	2.50	2.35	2.22	2.08	1.93	1.80	1.61	1.42	1.21	1.00
N	75	2.66	2.55	2.41	2.27	2.12	1.98	1.84	1.65	1.46	1.24	1.03
O	100	2.69	2.58	2.43	2.29	2.14	2.00	1.86	1.67	1.48	1.26	1.05
P	150	2.73	2.31	2.47	2.33	2.18	2.03	1.89	1.70	1.51	1.29	1.07
Q	200	2.73	2.62	2.47	2.33	2.18	2.04	1.89	1.70	1.51	1.29	1.07
		0.15	0.25	0.40	0.65	1.00	1.50	2.50	4.00	6.50	10.0	15.0
		Acceptable quality levels (tightened inspection)										

- All AQL values are in percent defective
- ↓ Use first sampling plan below arrow, that is, both sample size as well as k value. When sample size equals or exceeds lot size, every item in the log must be inspected.

There are two methods used in finding the variability of a lot when sampling per MIL-STD-414: the standard deviation method and the range method.

Standard Deviation Method

In this method, an upper and low Q value are calculated using a technique that is similar to that of determining a z-score for a probability distribution.

Q_U or $Q_L = \dfrac{\text{Specification Limit} - \overline{X}}{S}$ where S is the sample standard deviation and $\overline{X}$ is the sample mean.

Example:

The maximum height for a rod is specified as 6 feet. A lot of 100 is submitted for inspection. The inspection level is chosen as IV with an AQL of 1%. The lot standard deviation is unknown. Using this

information and the previous tables, the sample code is found to be F and n = 10 samples. The 10 readings are taken as follows:

6.1ft 6.25ft 6ft 6ft 6.2ft 5.95ft 6.05ft 6.1ft 6ft 6.15ft

$\bar{X}$ = 6.08ft and S = .13ft. The calculation continues:

$$Q_U = \frac{\text{Upper Specification Limit} - \bar{X}}{S} = \frac{6\text{ft} - 6.08\text{ft}}{.13ft} = \frac{.08}{.13} = 0.62$$

Since the number obtained 0.62 (actually -0.62, but an absolute value is used) is less than the K value of 1.72 in the table, the lot is rejected.

Range Method

To use the range method $\bar{R}$ must be determined first. $\bar{R}$ is the average range of the subgroups. If there is only one subgroup R, or the range of the single subgroup may be used.

$$Q = \frac{\text{Tolerance Limit} - \text{Mean}(\bar{X})}{\text{Average Range } (\bar{R})}$$

Similar to the last example, there are three different levels for inspection (as in MIL-STD-105E): normal, tightened and reduced. There are rules for each of these levels and the level must be defined for the sampling plan to be found. If it is determined that the sample size is greater than or equal to the lot size, every part in the lot must be inspected. The reader is referred to the standard itself and other texts for all procedures and any example calculations.

Random Sampling

Random sampling assumes that the selection of a single sample is truly random. That is to say that the selection probability for all possible samples has the same probability and that the sum of all possible sample probabilities totals to one. Random sampling requires that random numbers be generated and used to select the correlated product for sampling analysis.

Example:
For a computer generated two-dimensional array, the numbered rows and columns must correspond to the system of random numbers. For example, a array might consist of 8 columns and 6 rows. Then, using an algorithm, a random selection of numbers would determine a row and column to determine a specified location within the array.

Stratified Sampling

When the "lots" are combined from different machines, production shifts, operators, paths, etc., the process of selecting proportional samples from the various production shifts, machines, etc., is referred to as stratified sampling. Basically, an attempt is made to draw a random sample proportionately from each true by selecting a random, proportional sample from each "sub" lot.

- Sampling Bias. It should be noted that unless rigorous procedures are set up for sampling at random and/or by stratification bias(es) may be introduced which are detrimental to good decision making. For more detailed information on bias, the student is referred to the literature listed as references at the end of this section.

Example:
You inspect items which you receive in random order from five different production operators. Each operator produces 200 items which gives you a total lot of 1,000 items. As you receive the combined lot, you would separate it into sub-lots corresponding to the five operators' lots. Then, within each of the five sub-lots, you would employ random sampling to select the items for inspection. This process would enable an inspector to identify if problems exist with a particular operator or equipment within a specific assembly line.

Cluster Sampling

Clustering and discrimination methods are part of the area of statistics called *multivariate analysis*. Cluster sampling is useful in quality control when several different kinds of malfunctions within a production facility cause product to fall outside of engineering limits. It is often difficult to determine the causes of the malfunction in any one case, but clustering a number of the malfunctions may reveal causal links via common factors over the clusters. That is, this method

allows one to ask, “what do the cases with malfunctions of each type have in common?”

While the previous sampling methods are directed toward determining defectives within the *product*, cluster sampling’s goal is determining deficiencies in the *process*. Cluster sampling deals with investigating two or more consecutive steps within the overall process. At least one of the steps in the process – but not the first step – is the suspected deficient action within the process.

Cluster sampling is a form of time-series analysis. In the sampling process, clusters are examined to determine whether the deficient or problematic steps are related by virtue of improper or inadequate performance of the steps within the process. Typically, failures or deficiencies within the process are expected to be randomly distributed, but occasionally deficiencies occur in clusters. Cluster sampling will eliminate these “clusters by chance”.

Our examination of the cluster sampling process, also termed cluster analysis, will focus on maintenance actions within the process under review. In our example, the purpose of cluster analysis is to identify maintenance actions within the process that are caused by inadequate or improper performance of previous maintenance actions. The major steps of the process are:

1. Identify clusters which are the repetitive maintenance actions.
2. Determine whether the maintenance actions are related due to personnel performance problems.
3. Synthesize the results to help focus the diagnostic process to determine the programmatic root causes.

The principle underlying the cluster analysis approach is that the distribution of unscheduled maintenance actions will be typically random *if the maintenance actions are independent*. The random failures result in an exponential distribution of failures with time. This phenomenon applies to both electronic and mechanical systems.

Mechanical systems tend to exhibit a normal “wear-out” type of distribution for new systems, but eventually they exhibit the exponential distribution after replacement of many parts over a period of time so long as all the parts do not have the same wear-out rate. The replacement of different parts over time results in the system

being comprised of parts of varying age. This distribution of parts of varying age results in an overall exponential distribution of failures even though the underlying distribution of the mechanical parts subject to wear-out is normal (Gaussian).

The exponential pattern of failures results from *independently failing components* having a constant failure probability per unit of time, given that an equipment has survived to that time. *If a failure rate deviates from that pattern, with a greater number of short-time failures than expected, there is a strong indication that the failures are not independent.* Note that some short-time failures are expected, but the number of short-time failures will be small.

There are many factors that could cause the lack of independence of failures. For example, some failures may place undue stress on other parts and increase their failure rates. For the purpose of this project, the failures of primary interest are the failures (or unscheduled maintenance actions, to be more exact) that *are related by common personnel errors or other related maintenance problems*.

Example:

Step 1: Sort Data

If a database is used to maintain maintenance records, the following data fields should be available: equipment identified, equipment nomenclature, repair ordered date, repair start date, repair completion date, problem description, and work description. The database should be sorted by equipment identifier and repair ordered date.

Step 2: Identify Clusters

It is possible to identify clusters by considering two or more maintenance actions as part of a cluster when an equipment identifier appears more than once *and* the initiation date of the second or later actions is later than the repair date of the first action. If the second work order was initiated before repair was started on the first work order, the two actions should not be considered as a cluster.

Step 3: Determine Relevant Clusters

This is done by examining the problem description and work description to determine whether the later maintenance actions were caused by an earlier maintenance action. In some cases, the

relationship is quite clear – for example a wire left unattached or only three of four bolts installed. Other relationships such as leaky valves or connectors are more difficult to determine. In some cases, it may be necessary to interview the technicians or engineers involved with the work order.

Step 4: Group Clusters into Categories.

Once a cluster is determined to be relevant, the apparent performance problems are grouped into categories with similar performance characteristics, e.g., inadequate diagnosis, improper tightening of fasteners, etc. Such categories make it easier to determine the programmatic root cause. It is essential to ensure that all the clusters in the group seem to have the same programmatic root cause.

Step 5: Determine Consequences of Relevant Clusters

When outages or power reductions are involved, the consequences should be expressed in those terms. When there is a known impact on safety, the safety impact should be stated. Consequences on man-hours should also be expressed when applicable.

Step 6: Determine Technicians Involved

At this stage of the analysis, the data will not indicate the number of technicians involved per problem area. Such data is useful in diagnosing the programmatic root cause. If the source data does contain the names of technicians involved, you should determine their number and the percentage of similar tasks, e.g., 50% of valve packing performed by one-third of the technicians. The purpose of this step in the analysis is to determine how to improve the performance of technicians by improving their support in terms of procedures, documentation, or training.

Characteristics of Good Sampling Plans

The following are general guidelines to be followed for sampling:

- A sampling plan should take advantage of known information such as a documented process average, process capability, etc. so as to minimize redundancy in analysis thereby minimizing sample inspection and analysis costs.
- A good sampling plan should be simple, understandable and easy-to-follow for management, the administrator and inspectors.

- The desired sampling variables should be known and compatible with the end product's or the consumer's priorities or desired attributes.
- The chosen quality index (AQL, AOQL, LTPD, LQL, etc.) should reflect the needs of both the producer and customer.
- Sampling plans should be selected based on their value to provide an on-going evaluation of process performance wherever possible.
- Sampling plans should be designed to have flexibility to reflect changes in desired quality and quantity of production.

References and Suggested Reading

Juran, J. M., Quality Control Handbook, McGraw-Hill, Inc. New York, NY, 1988.

McClave, J. T. and Dietrich II, F. H., Statistics, Dellen Publishing Company, San Francisco, CA, 1985.

Speigel, M. R., Schaum's Outline Series: Theory and Problems of Statistics, McGraw-Hill, Inc. New York, NY, 1995.

U.S. Nuclear Regulatory Commission, Programmatic Root Cause Analysis of Maintenance Personnel Performance Problems (NUCREG/CR-5666), NRC, 1991.

Wortman, B., Certified Quality Engineer Primer, Quality Council of Indiana, West Terre Haute, IN, 1995.

References and Suggested Reading

Problem Analysis and Risk Assessment Terminology

Section 2

OBJECTIVE

Demonstrate knowledge of terminology associated with probabilistic risk assessment (PRA) techniques

2 - 1

1. Define the following terms with respect to probabilistic risk assessment (PRA):

- **Probability**
- **Reliability**
- **Availability**
- **Unavailability**
- **Risk**
- **Safety**
- **Accident Sequence**
- **Dominant Contributors**
- **Minimal Cut Set**

Probability

Probability is the likelihood of the occurrence of an event.

Reliability

Reliability is the probability that a product will perform its intended function satisfactorily for a pre-determined period of time in a given environment.

Availability

Availability is a measure of the degree to which an item is in an operable and committable state at time *t*.

Three common measures of availability are:

1. Inherent Availability (A_i)
2. Operational Availability (A_O)
3. Achieved Availability (A_A)

1. Inherent Availability (A_i)

   This is the ideal state for analyzing availability. The only considerations are mean time between failure (MTBF) which is a measure of reliability and mean time to repair (MTTR) which is a measure of maintainability. This measure does not take into account the time for preventative maintenance and assumes repair begins immediately upon failure of the systems. The measure for inherent (potential) availability (A_i) is $A_i = \frac{MTBF}{MTBF + MTTR}$.

2. Operational Availability (A_O)

   This is the measure of availability that generally occurs in practice. It assumes that the maintenance response is not instantaneous, parts may not be in stock for repair, and/or other logistics issues impact the time before maintenance response is initiated. The measure of operational (actual) availability (A_O) is $A_O = \frac{MTBMA}{MBTMA + MDT}$.

   MTBMA = mean time between preventive and corrective maintenance actions
   MDT = mean down time

3. Achieved Availability (A_A)

   Achieved availability is still more realistic since it includes preventative maintenance as well as corrective maintenance. As in A_i, A_A assumes that no time is lost waiting for the maintenance action to begin. The measure of achieved or final availability (A_A) is mean maintenance action time (MMT). MMT is decomposed into the effects of preventative and corrective maintenance and is given as

   $$MMT = \frac{F_C \bar{M}_{ct} + F_p \bar{M}_{pt}}{F_c + F_p}.$$

   F_c = number of corrective maintenance actions per 1000 hours
   F_p = number of preventative maintenance actions per 1000 hours
   M_{ct} = mean active time for corrective maintenance (MTTR)
   M_{pt} = mean active time for preventative maintenance

Unavailability

Unavailability is the probability that a component is in a failed state at time *t* given that it was good as new at *t = 0*.

Risk

Risk describes both the probability and the consequence of a loss event. In other words, Risk = Probability × Consequence. Consequence can also be termed *severity*, and it refers to the magnitude of the loss in a given period of time.

The assumed effect of an uncontrolled hazard is the combination of:

- the *probability* it will happen
- the maximum *severity* of any injuries or damages
- the public's *sensitivity* to the occurrence

A dictionary term of risk is "the *possibility* of loss or injury to people and property." A PRA definition of risk is "the *probability* and *severity* or *magnitude* of loss or injury to people or property. Severity or magnitude are synonyms for consequence. The PRA risk equation becomes Risk = Probability × Magnitude. The three terms can be further refined as:

Risk	Probability	Magnitude
$\frac{\text{consequence}}{\text{time}}$	$\frac{\text{events}}{\text{unit time}}$	$\frac{\text{consequence}}{\text{event}}$

Example:
If there are 20,000,000 industrial accidents in the world every year and the consequence (deaths per accident) is 4×10^{-4}, compute the annual industrial accident death rate.

(20,000,000 accidents/yr) x (4×10^{-4} deaths/accident) = 8,000 deaths/yr

Safety

Safety is the elimination of hazards or the control of the hazards to levels of acceptable tolerance. A hazard is the source of energy and the physiological and behavioral factor which, when uncontrolled, leads to harmful occurrences.

A design engineer concerned with mechanical loading devices must consider the *safety factor* and *margin of safety*. These are defined as:

$$\text{Safety factor} = \frac{m_x}{m_y} \qquad \text{Margin of safety} = \frac{m_x - m_y}{m_y}$$

μ_x = average strength
μ_y = average stress.

Example:
An aluminum tank is being designed with an average material strength of 300 psi. The expected stress is 140 psi. What is the safety factor? What is the margin of safety?

SF = 300/140 = 2.143 or 214.3%

MOS = (300-140)/140 = 1.14

Accident Sequence

A typical probabilistic risk assessment consists of the evaluation of accident sequences: initiating events followed by combinations of successful and unsuccessful responses of structures, systems, components, or operator actions. Each (unique) accident sequence is defined by its event failures and labeled by the appropriate designators. Event tree models (bimodal logic diagrams) are constructed to logically represent the above combinations of functional, systemic, and operator responses to the initiating events. Each unique set of failure responses is called a sequence.

Dominant Contributors

Dominant Contributors are those accident sequences, starting with the highest risk in terms of quantified values that ,when summed, encompass a majority (usually $\geq$ 90%) of the risk associated with the given facility or system being analyzed. For example, loss of off-site power combined with failure of the emergency diesel generators has been shown to be dominant contributors at some boiling water reactor nuclear facilities.

Minimal Cut Sets

In a fault tree, top event or individual system failure modes are defined by failure of one or more events; this forms the basis for the concept of a *cut set*. A cut set is one or more basic events, which, if they occur, the top event (“tree top”) is guaranteed to occur.

Large systems have an enormous number of components and each may posses numerous failure modes. As a result, where complex systems contain hundreds of components and dependencies, hundreds of thousands to hundreds of millions of cut sets are possible. This essentially says that there are numerous of ways to reach the same

type of failure. Therefore, it is desirable to reduce the number of cut sets we must analyze to simplify the analysis. We require only those failure modes or combination of events which are unique and are not duplicated by the addition of another basic event to a series of events that already lead to failure. The latter is demonstrated by an example below. No useful information is lost by this restriction. Note however, if it were possible to improve or redesign and construct the system so as to eliminate all the “unique” failure modes, all the duplicative system failure modes would also be eliminated.

The above discussion of a unique (and minimum) combination of failure events defines the *minimal cut set* concept. As such, a minimal cut set is such that if any basic event is removed from the set, the remaining events collectively are no longer a cut set, or stated another way, if any basic event were removed there would not be failure of the top tree event. Defining this concept in a fault tree solution algorithm allows us to reduce the number of basic events required for top tree event failure, and therefore the number of cutsets needed to be analyzed.

Example: Consider two valves in series on an injection line path to the core of a reactor. If the valves are normally closed and are opened upon actuation, failure of either or both to open would defeat the injection path. In minimal cutset space, the failure of both to open is not a minimal cut set and is therefore eliminated from consideration since the failure of either valve to open defeats the injection path.

2. Define event tree and fault tree; differentiate between the associated processes.

2 - 2

A. Event Trees

Event trees are system level logic diagrams. A single tree represents the combinations of system and operator response successes and failures that lead to unique sequences of events following a specific initiator such as loss of offsite power. The tree then depicts the various system level and operator responses designed or procedurally directed to address to the initiating event. This process forms the basis for the name Accident Progression Event Tree (APET) which is often associated with event trees for accident analysis.

Event trees are used to define accident sequences that involve the complex interrelationships among engineered safety systems. They are constructed using *forward or inductive logic* and generally seek to model structures, systems, components and operator responses as a result of an initiating event. As an example, suppose the initiator is a loss of offsite power, in this instance you would ask “What happens as a result of a loss of offsite power (LOSP)”? One such response could and generally would be an automatic start of an onsite backup or emergency diesel generator. The development of fault trees addressing the probability of events designed to respond to the LOSP are performed using *backward or deductive (fault tree) logic* and by asking the question “How could a loss of offsite power be mitigated?” An example would be asking “What combinations of events could cause the emergency or backup diesel generator power to fail?” and then constructing a fault tree for the emergency diesel generator electric power subsystem. Then, the frequency for a site or facility blackout (loss of both onsite and offsite power) could be obtained by multiplying the initiator frequency for LOSP by the probability of failure to provide emergency diesel generator backup power.

Event Tree Process

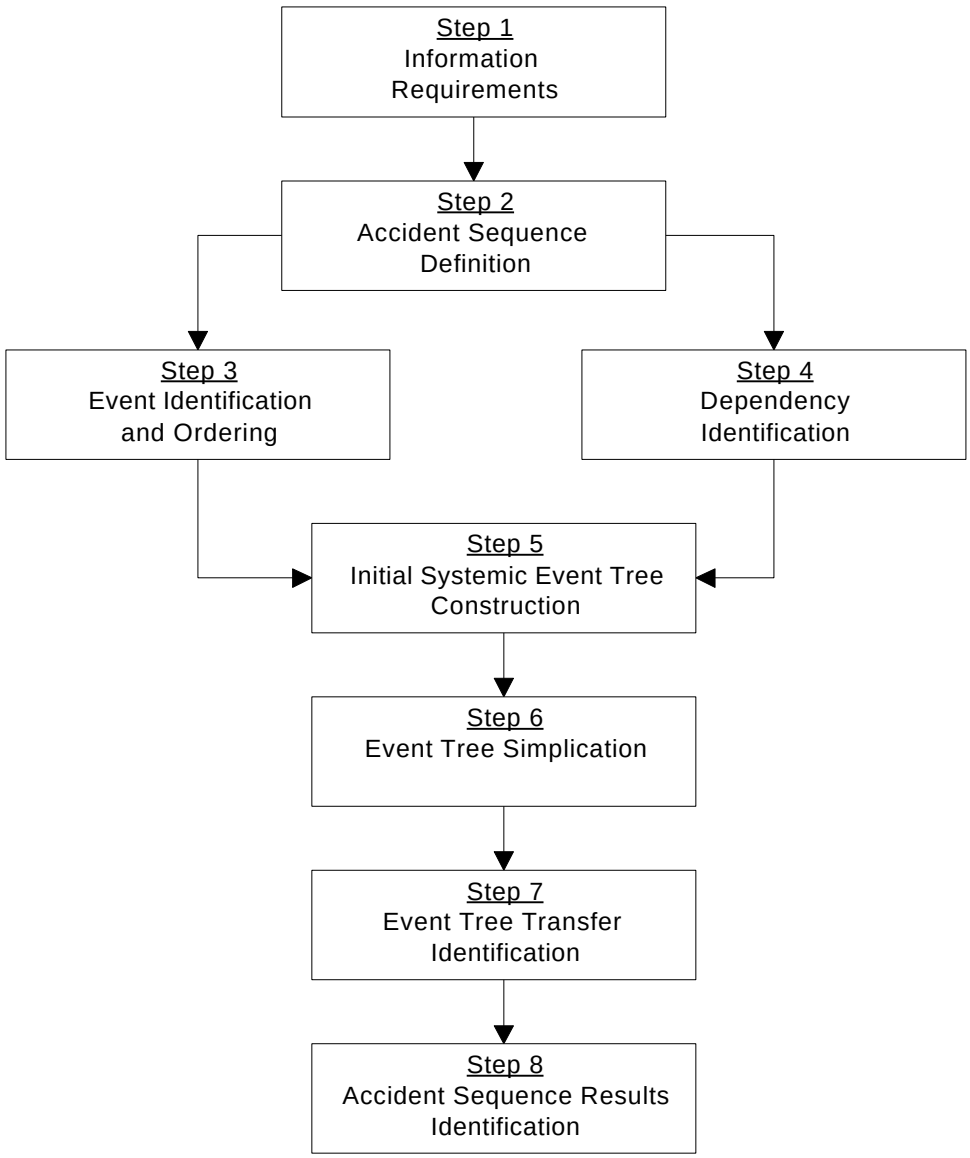
The construction of the event trees involves several steps that are illustrated in Figure 2.1.

Step 1: Information Requirement

Before actual development of the event tree commences, certain information needs to be gathered that is the product of previous tasks. Examples of this information might be the list of LOCA and transient initiating event groups, success criteria for LOCA and transient initiating event groups, and various plant information.

Event Tree Process

Figure 2.1



Step 2: Accident Sequence Definition

Before event tree headings (top events) are identified, the different end states of the accident sequences need to be defined. The philosophy behind event tree analysis is to depict system successes and failures until it is resolved that release occurs and to display the status of other systems sufficient to describe the state of the plant for containment and consequence analysis. The event tree developed reflects responses that can potentially mitigate core damage and containment failure and also influence the consequences of the accident sequences.

Step 3: Event Identification and Ordering

Each event tree has specific systems or groups of systems as the heading. The heading or system top events are identified from the success criteria.

Step 4: Dependency Identification

The dependencies among the set of system events on the event tree for each initiating event are identified in this step. As each top event is sequentially encountered in the event tree, the analyst must consider the status of all top events that preceded it. There are three types of system-level dependencies that need to be considered:

- The system either succeeds or fails by definition because of the previous success or failure of another system or set of systems.
- The system fails because of an expected phenomenological occurrence associated with the accident sequence.
- The success or failure of the system does not affect the potential for core damage or reduce the consequences expected because of the success or failure of other systems in the accident sequence.

Step 5: Initial Systemic Event Tree Construction

A draft systemic event tree is constructed using the front-line system events identified as event tree headings in Step 3 and incorporating the dependencies identified in Step 4. The dependencies are incorporated in the tree structure by removing success or failure decision branches that result in an inconsistent sequence. An event tree is constructed for each initiating event. Therefore, each tree has a unique structure that reflects the different mitigating system requirements that were the basis for the grouping of initiating events.

Step 6: Event Tree Simplification

The event tree is reviewed to ascertain whether the structure could be simplified while retaining system dependencies if the order of events are changed. This step is performed if simplification significantly reduces the number of resulting sequences and thus decreases the quantification process. Additionally, if the analyst can determine that the frequency of a

partially developed sequence is significantly less than that of other sequences, it need not be further developed.

Step 7: Event Tree Transfer Identification

In some cases, after the initiating event and subsequent success or failure of other events, the accident *looks* like a different initiating event accident and thus requires different success criteria than the initial event. The sequence could then be transferred to that tree, or it might require an entirely new event tree.

Step 8: Accident Sequence Results Identification

Each accident sequence is defined by its event failures and labeled by the appropriate designators. Each accident sequence is consecutively numbered and identified.

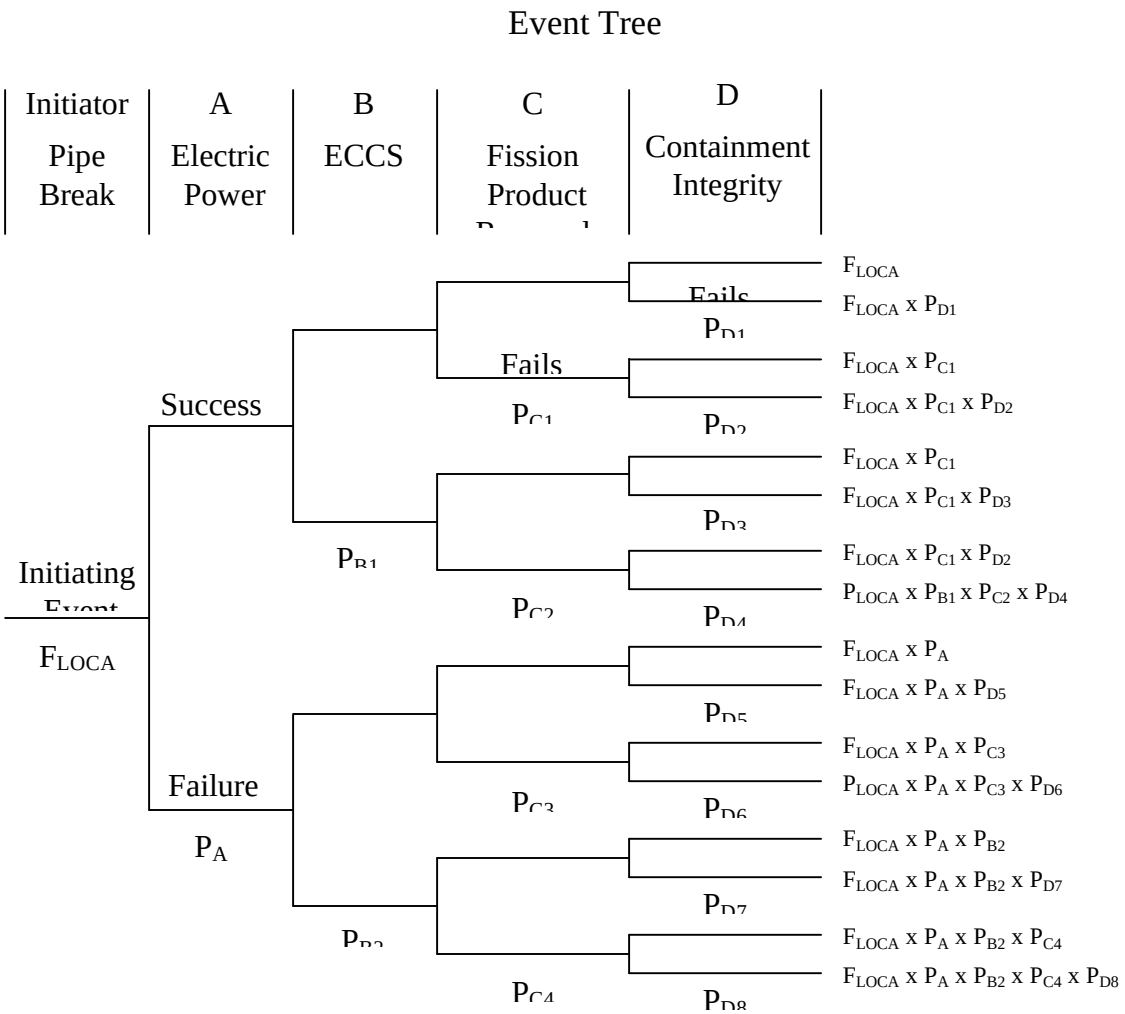
Event Tree Construction

The following is a simplified example for a reactor safety study where the risk associated with the accident is radioactive (toxic) fission product release.

The first step in event tree construction is to identify the various means or paths through which a release might occur. This process defines the accident sequences that would need to be quantified. The *initiating event* for a pipe break has a frequency designated as F_{LOCA}. This frequency is generally expressed as a probability per year for a coolant pipe break or $F_{LOCA} = P_{LOCA}$ /year.

A simplified event tree for a loss of coolant accident (LOCA) in a typical nuclear power plant is shown in Figure 2.2. The accident starts with a pipe break having a frequency of F_{LOCA}. The simplified course of events that might follow a LOCA are then examined. For this example, the event tree displays simple alternatives or decisions with associated path outcomes.

Figure 2.2

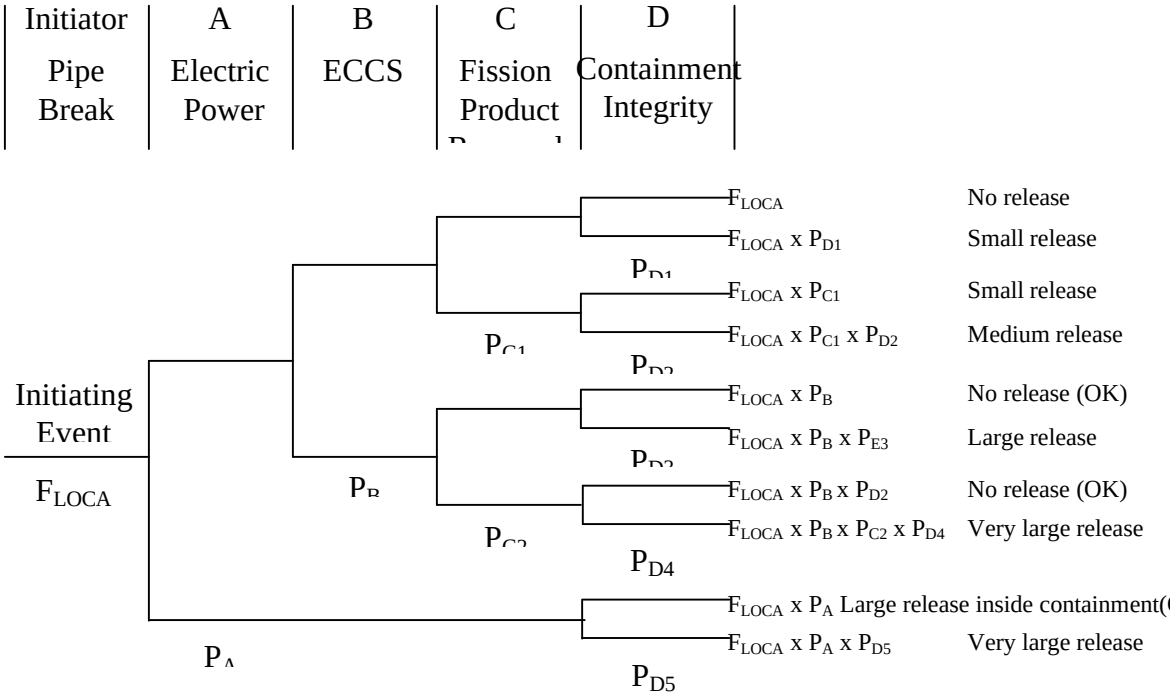


Generally, the event tree process is a binary analysis where a structure, system, component (SSC), or operator action either succeeds or fails. The resulting number of potential accident sequences is 2^{N-1} where *N* is the number of event tree tops (excluding the initiator) representing the SSCs and decisions being considered. For the purposes of this example, and in general, the basic tree may be pruned to the reduced tree shown in Figure 2.3 by recognizing obvious interrelationships between previously failed SSCs and subsequent SSCs. As an example consider the failure of electric power after the pipe break. Upon failure of the electric power system the Emergency Core Cooling System (ECCS) system would not have power available to start and operate the ECCS pumps. Nor would there be much likelihood of operation of the Fission Product Removal systems assuming active systems that require power. However, containment integrity could and probably would function,

so we only need ask the question concerning containment integrity following the failure of electric power. Essentially following the failure of electric power, the question becomes what is the probability P_C, of ECCS failing given F_{LOCA} and P_B and how would it affect the remaining safety systems? The pruned tree shows this and other similar simplified choices when electric power and other systems are unavailable.

Pruned Event Tree

Figure 2.3



By working through the entire event tree, we produce a spectrum of release magnitudes and their frequencies for the various accident sequences.

In Figure 2.3, the sequence *end states* are currently expressed in terms of the product of the initiating frequency multiplied by subsequent failures that eventually lead to the release of radioactivity to either the inside or outside of the containment. Usually in the case of a reactor analysis, end states are generally expressed in terms of an undesirable release to the environment outside of containment. Consequently, and as demonstrated by sequence F_{LOCA} x P_A even if there is a large release within the confinement, the outside environment is not affected as long as confinement integrity is intact. As a result, this sequence results in an “OK” end state label.

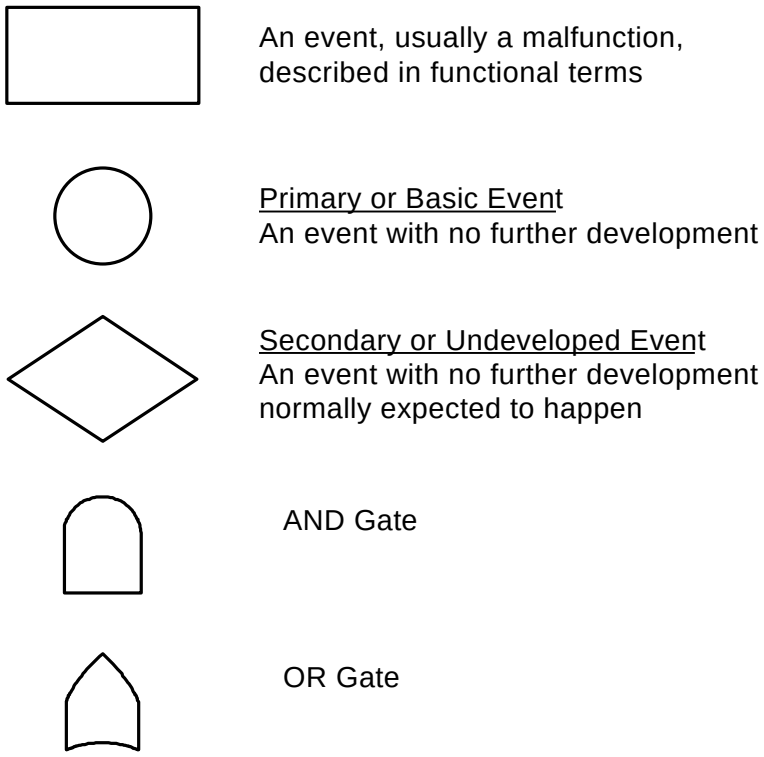
Each event tree top failure must be modeled to allow for sequence quantification. This process of modeling is commonly referred to as a fault tree. The next section discusses this process in detail.

B. Fault Trees

Fault Tree Analysis (FTA) is a symbolic logic diagram which graphically shows the various combinations of equipment failure and operator errors that may lead to failure of the top event. A FTA uses the basic symbols in figure 2.4 (page 2-12) as well as others to develop a logical model of an event tree top failure. Consequently, the top event of a fault tree and the event tree decision branch (normally across the top of the event tree as in figure 2.3) represent the same failure. The fault tree is normally the method by which each event in the event tree is quantified.

Figure 2.4

Basic Fault Tree Symbols



Using these symbols, a fault tree is constructed using three steps. The first would be the determination of the head event from the event tree top developed from the accident progression event tree. The second is the development of the intermediate events representing the various means (at a high level) by which failure of the top event can occur. The final step is the development of the relationship between the causal events or basic events and the event tree top using AND and OR logic gates.

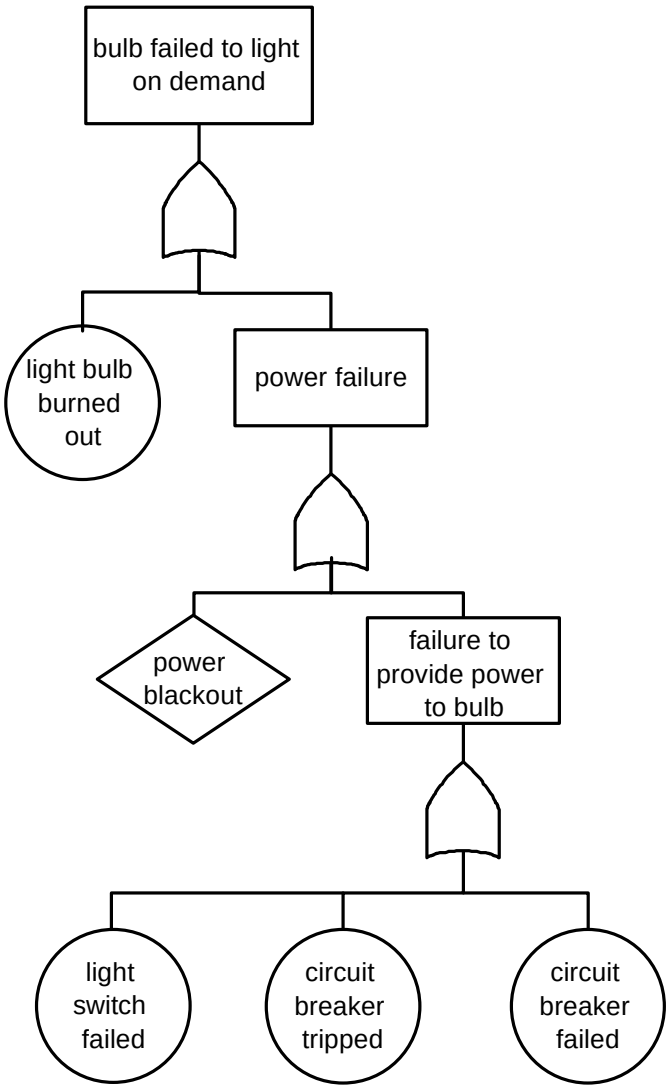
An example of a simple fault tree may help explain how AND and OR logic and basic events are used to define logical failure relationships. If a simple analysis is done on the failure of an electric light bulb to produce light upon turning the switch on, the fault tree depicted in Figure 2.5 can be developed.

The tree shows three OR gates. Upon failure of the light to light, there are two possible causes: either the bulb has burned out*or* there has been a power failure (both developed events). If there has been a power failure, there are two different causes: either there has been a power outage (a blackout) shown as an undeveloped event *or* there has been a failure to provide power to the bulb (developed event) with three basic event failures as inputs into the event.

If on the other hand, there had been a need for an AND gate and it was placed as a developed event below the power failure, both a power blackout and a failure to provide power to the bulb would be necessary for the bulb failed to light on demand event to happen.

Figure 2.5

A Simple Fault Tree



References and Suggested Reading

References and Suggested Reading

Drouin, M. T., Harper, F. T., Camp, A. L., Analysis of Core Damage Frequency from Internal Events: Methodology Guidelines, Volume 1, U.S. Nuclear Regulatory Commission, Washington, D.C., 1987.

Grimaldi, J. V. and Simonds, R. H., Safety Management, American Society of Safety Engineers, Homewood, IL, 1989.

Henley, E. J. and Kumamoto, H., Probabilistic Risk Assessment, The Institute of Electrical and Electronics Engineers, New York, NY, 1992.

Kohn, J. P., Friend, M. A., and Winterberger, C. A., Fundamentals of Occupational Safety and Health, Government Institutes, Inc., Rockville, MD, 1996.

Risk Assessment

Section 3

OBJECTIVE

1. Demonstrate the ability to apply principles of risk management in preparing a risk assessment project.

2. Demonstrate the ability to participate in the preparation of a risk assessment for the project plan of a major system acquisition (MSA), major project

3 - 1

1. Demonstrate the ability to apply principles of risk management in preparing a risk assessment for a project.

The concept of risk management is rooted in the public's concern over its safety which may be impacted by the hazards of daily routine and occupational hazards, including all industrial and nuclear facilities which may have an impact either directly or indirectly upon the public. As the risk of death resulting from these hazards approaches 10^{6}/year, public concern reduces to a point where no undue cautions are taken to avoid the accident. As such, most individuals do not live in fear of being struck down by lightening which has a risk level of approximately 10^{-6}/year.

The process of risk management as it applies here then seeks to reduce public risk as a result of direct exposure to the hazards of industrial and nuclear facilities to an acceptable level, namely an early fatality rate approaching the 10^{-6}/year level. The process essentially consists of reduction in the occurrence of catastrophic events through analysis and implementation of engineered design and siting requirements, procedural compliance, maintenance specifications, training and qualification requirements/standards, operating and safety limits and associated protective systems, accident mitigation, and defense-in-depth barriers designed to prevent or minimize release of hazardous byproducts associated with facility operation.

Historically, the DOE and other governmental agencies have applied this process extensively to nuclear and some non-reactor nuclear

facilities and a few other high hazard facilities/programs (i.e., space programs). Many of the efforts to date have been focused on facilities where it may be perceived that there are unacceptable psychological or social risks rather than the actual risk of early fatality. This may be attributed to an observation that mortality risk due to voluntary exposure (i.e., driving a car) is a factor of 10^3 higher than for involuntary exposure (i.e., having a nuclear or high hazard non-nuclear facility sited in near proximity to one's home or work). This generally says that an industrial or a nuclear facility must be designed to be 1,000 times safer than a car.

Another factor in this equation is that of consequence. In the case of an accident involving a car, the consequences are generally localized to involve those occupying the vehicle or vehicles involved in the accident, while for the industrial facility, the impact may extend out into the public at large. The best example of this is the Bhopal, India chemical release accident where thousands were killed as a result of a deadly gas cloud released from the plant. Therefore, when the consequences of a single accident generally extend into the public at large, the accident is viewed as unacceptable.

The information in Table 3-1 is taken from WASH-1400 and depicts the individual risk of early fatality by various causes to an individual within the United States. Except for the numbers for hurricanes, tornadoes, and nuclear accidents, all numbers are based on the total population. For tornadoes, the numbers are based on a 1953-1971 average and similarly for hurricanes, a 1901-1972 average. For nuclear accidents, the risk is based on a population (at risk) of 15 million.

Table 3.1

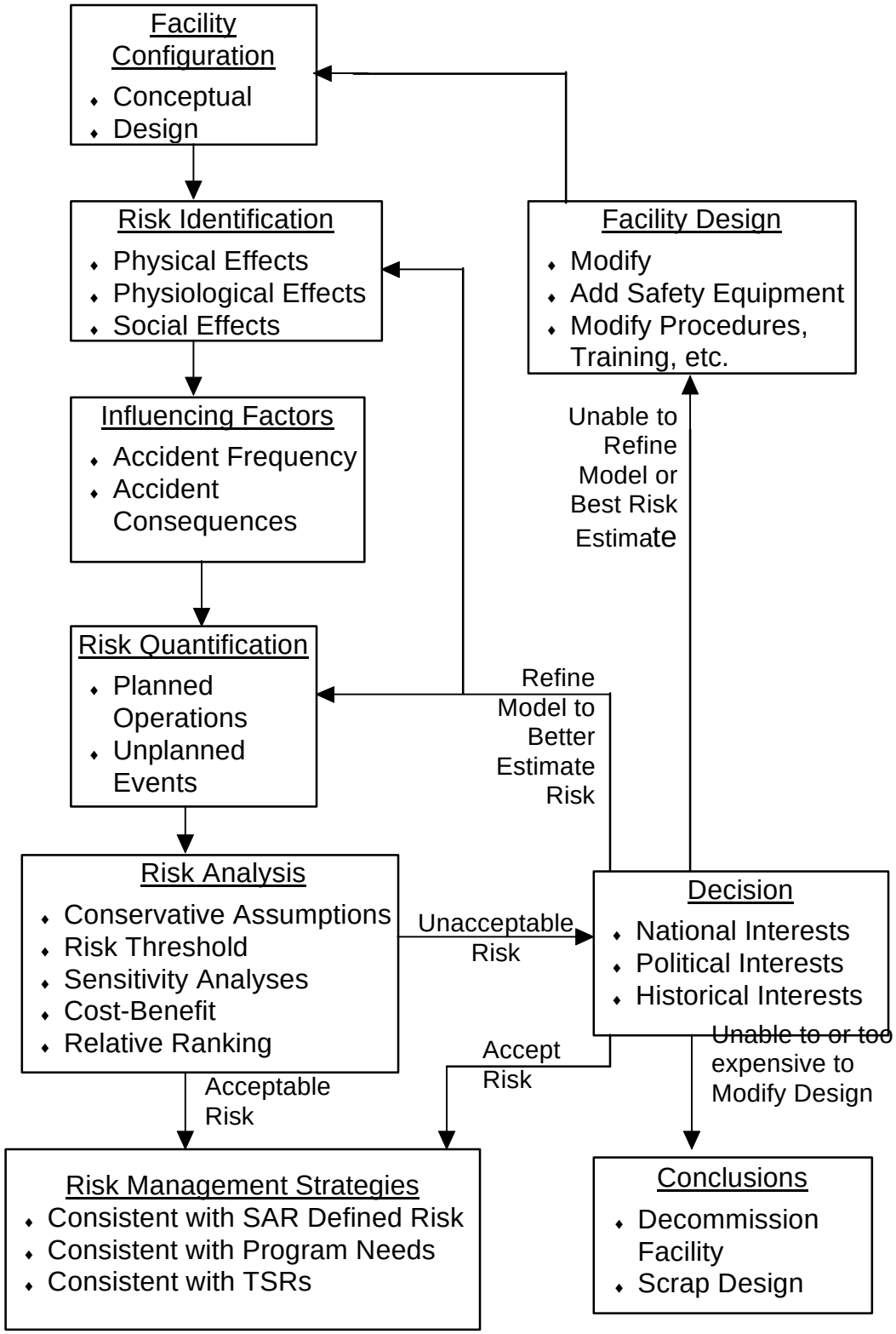
Individual Risk of Early Fatality by Various Causes

Accident Type	Approximate Individual Early Fatality Risk (Probability/year)
Motor Vehicle	3×10^{-4}
Falls	9×10^{-5}
Fires and Hot Substance	4×10^{-5}
Drowning	3×10^{-5}
Poison	2×10^{-5}
Firearms	1×10^{-5}
Machinery (1968)	1×10^{-5}
Water Transport	9×10^{-6}
Air Travel	9×10^{-6}
Falling Objects	6×10^{-6}
Electrocution	6×10^{-6}
Railway	4×10^{-6}
Lightning	5×10^{-7}
Tornadoes	4×10^{-7}
Hurricanes	4×10^{-7}
All Others	4×10^{-5}
Nuclear Accidents (100 Reactors)	2×10^{-10}
All Accidents	6×10^{-4}

The process of risk management within the DOE essentially reduces to Figure 3.1 which summarizes the process.

Figure 3.1

DOE Risk Management Framework



3 - 2

2. Demonstrate the ability to participate in the preparation of a risk assessment for the project plan of a major system acquisition (MSA), major project (MP), and other project (OP).

A. Assess project risks that identify critical systems, subsystems, and other factors that require focused work and resolution.

The process of assessing project risks to identify critical systems, subsystems, and other factors requiring focused work and resolution consists essentially of the following:

- Identify the hazards.
- Identify the parts of the process or system that give rise to the hazards identified.
- Establish the scope of the study. (Will it include earthquakes, tornadoes, flooding, internal failures, sabotage, etc.?)
- Identify all Category 1 and 2 hazards.
- Identify all active systems, barriers, components, and other passive design features needed to address or mitigate Category 1 and 2 hazards.
- Prepare a Preliminary Hazards Analysis (Optional).

The technique used to perform a Preliminary Hazards Analysis (PHA) is discussed in more detail in Section 5. Generally, qualitative and lesser quantitative techniques are used to arrive at a hazard determination as defined by the following hazard category levels:

- Category 1: Hazards show significant offsite consequences
- Category 2: Hazards show significant onsite consequences
- Category 3: Hazards show only localized consequences

The end result of this process is the identification of those structures, systems, components, and any other factors that are required to mitigate or control unacceptable hazards and thereby maintain acceptable risk levels.

B. Evaluate the assessed level of risk.

The next step in the process is to quantitatively evaluate the risk associated with the hazards and mitigation or prevention processes previously identified above as a Category 1 (and sometimes 2)

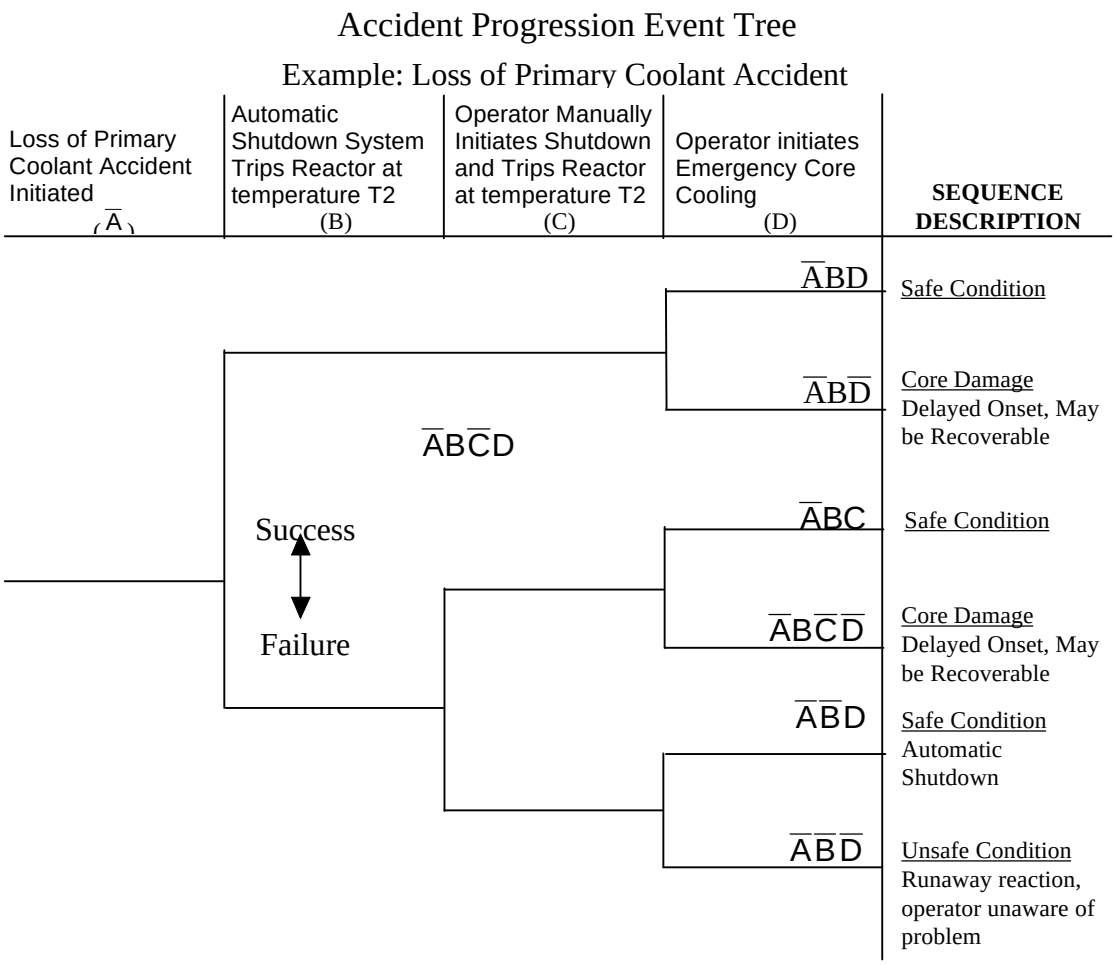
hazard. One of the most widely used processes generally involves the use of fault tree/event tree methodology where accident progression event trees (APETs) are developed during and upon completion of the facility/system design phase/process.

Another methodology for evaluation of the risk is through the use of a Failure Modes and Effects Analysis (FMEA). This methodology is less rigorous than the fault tree/event tree methodology and generally is used when a simplified, lower cost, scoping analysis is desirable. The FEMA technique is further discussed in section 5. The fault tree/event tree methodology is most commonly used within the DOE when addressing complex Category 1 hazards (and some category 2 hazards), and it will be the basis for further discussion.

The process of evaluating the level of risk using event tree and fault tree methodology is developed from the previous analysis where Category 1 and 2 hazards and associated preventive and mitigative systems were identified. Following the initial identification of the hazards, the hazards must be tied to initiators where an event either internal or external to the plant can create the conditions that will lead to the hazard to be analyzed. All “initiators” for a single or a similar group of hazards must be identified and summed to create a single accident initiator frequency.

Example:
One system that contains high energy fluid (and therefore a hazard) is the primary coolant system in a reactor. A pipe break would be an example of how the energy from within the pipe could be released to the surroundings. Therefore, the pipe break would represent an initiator for release of the high energy fluid. At this point the hazard has become an accident since it may ultimately lead to fuel damage and release of radioactive byproducts to the surrounding environment, hence the name accident progression event tree (APET). The pipe break may be initiated a number of different ways including an existing crack or pipe material flaw, a broken weld, or a broken flange seal, etc. All of these pipe failures would be grouped into an initiator of a loss of coolant. Following this, a number of questions are asked in order to better define the condition of mitigative SSCs designed to prevent or minimize the effects of the accident. These questions form the APET tops for the simplified example shown below in Figure 3-2.

Figure 3.2



The tops of the APET are quantified through the use of fault trees, and Boolean algebra is then used to combine and reduce fault trees using computer based algorithms. Occasionally, the event may be quantified by a simple yes/no or binary action/event. It is the combination of failure and success probabilities that leads to definition and quantification of accident sequences and forms the basis for probabilistic risk/safety analysis. This process can be time consuming and expensive when detailed analyses are required to support risk quantification of complex interactive SSCs. Where less rigorous treatment is warranted, the use of FMEA techniques may be employed.

C. Describe the basis for the risk assessment.

The basis for the risk assessment is normally the final facility or system/process design and equipment configuration (as-designed/ as- built). In addition, the basis includes the scope of the analysis and may include such considerations as siting in the form of analysis of earthquakes, external events such as tornadoes, hurricanes, fire, loss of offsite power, or flooding and, internal events such as fires, flooding, equipment failures, etc., the use and validity of data used in the analysis process, and any assumptions made during the analysis process. Often times, these techniques may be used to compare the safety design versus cost for a proposed new facility or process. Under all circumstances, the basis for a single risk assessment is rooted in its scope, the final design analyzed, the validity of any data used, and any assumptions made in the analysis process. All of these must be documented in a discussion of the analysis(es) in order to establish the basis and validity for the risk assessment.

D. Identify the critical project elements that contribute to risk.

This section of analysis involves the reduction of the accident sequences into a subset of those primarily responsible for the majority of risk. The process includes quantification of **all** accident frequencies combined with accident consequences through the use of computer risk analysis methods (fault tree/event tree sequence solutions). The consequences portion of this process attempts to bound the acute (and often times latent) fatalities expected to an individual of the general public resulting from exposure to the effects of an accident.

Upon completion of quantification as described above, those elements (basic events) that contribute the most to the quantification of risk may be identified by analyzing and displaying the results from the accident analysis according to individual event contribution. This process identifies *dominant contributors to risk* and in effect it sums up all cut sets containing the same factor or *basic event*. The process then identifies those events that are the largest contributors to risk across the spectrum of accident sequences analyzed.

Additional sensitivity studies are often performed whereby key SSCs or project elements are identified by setting their failure probability to 0 (reliability of 1.0), re-solving all accident sequences, and observing the quantitative effect on the overall risk (risk reduction measure). Conversely, the failure probability may be set to 1.0 (reliability of 0)

and its effects on risk observed (risk increase). These processes are often used to identify SSCs that are important to risk. For a more detailed discussion of the properties and meaning of these and other measures, the student is referred to Probabilistic Risk Assessment by E. J. Henley and H. Kumamoto.

E. Identify the consequences of an accident.

The identification of the consequences of an accident is generally performed following quantification of an accident frequency. In the first step of an accident analysis, only the frequency of accident occurrence is quantified. This is to allow the grouping of similar accidents that would be expected to have similar consequences prior to the analysis of consequences. Fundamentally this step is performed in order to reduce the amount of effort necessary in the analysis of consequences. The process of combining accidents into groups with similar consequences is normally referred to as “binning” of accidents. Generally, the consequences are arrived upon through another fault tree/event tree analysis of the statistical amount and duration of a defined type of hazard (a single “bin”) received by the public (or a worker if desired) with the received amount being compared against known lethal limits, or in the case of radiation or toxicity doses, a defined lethal dose where a given percentage of the population will die within a defined time period.

Example:
The acute whole body lethal dose for 50% (of the public) within 30 days of an exposed population for external exposure to radiation is defined as 200 rem. Received exposures may be compared against this number and its associated statistical curve to determine probable deaths that would result from a major radioactive cloud released such as could result from a reactor meltdown accident with a containment breach. This process may also be reduced to a dollar value associated with the risk where death is not expected but permanent or temporary incapacitating injury, or quality or length of life impacts are expected (e.g., loss of an eye, a finger, etc.)

F. Describe the influence the following parameters have on the results of a radiological consequence analysis.

In a radiological consequence analysis, the factors that influence the effects of an accident include: ***the amount and type (the elemental,***

chemical, and physical makeup of the source material) of radiological material dispersed, or the quantity of source material, the locally influenced environmental factors that determine the type and amount of release, the energetics or kinetic energy of the accident, the population density of the surrounding site, and weather conditions at the time of and following release.

These factors are discussed individually in the following subsections.

The amount and type of radiological material disbursed

This factor reduces to the simple statement that more is worse. This is a simplification but it is generally used in conjunction with the type of material. With certain types of releases, there are more severe consequences. As an example, radiological material released as a result of a burn results in a finer particulate disbursal than the same amount of material disbursed as a result of an explosion. The hazards of the fire disbursal can include entry into the body through ingestion and inhalation. Both of these paths are significantly reduced or eliminated from an explosive disbursal. Another example is the toxicity of the material. For a release of plutonium, toxicity considerations must also be considered. Plutonium powder is highly toxic and must be handled carefully. In practice, plutonium powder is always handled inside gloveboxes. For uranium and uranium powder, this is not as important since the toxicity is not a factor.

The locally influenced environmental factors that determine the amount and type of release

Following a release of radiological materials to the surrounding environment in the form of a fire, dispersion of aerosols or fine particulate, or a gaseous or liquid vapor, the amount and type of material released may be influenced by the presence of safety systems and other factors surrounding the accident location. As an example, following a release, the use of sprays or particulate filters on ventilation paths may be employed so as to minimize the release of particulate and aerosols to the surrounding (public) environment. Another such factor would be the use of catch tanks on contaminated drain systems that may be used to route released liquid materials to controlled locations. Finally, such mechanisms as plateout and other types of chemical reactions/interactions with surrounding equipment and structures may also influence the

amount of material that is ultimately released to the surrounding (public) environment.

The energetic or kinetic energy of the accident
The disbursal of material and particularly larger solids is primarily based upon the initial energy of release. This is particularly true when accidents occur with nuclear weapons but do not involve a nuclear yield. Under these circumstances, the amount and location of high explosive in proximity to the amount of nuclear fissile material will ultimately determine the amount of fragmentation and disbursal of nuclear material.

An additional factor would be the type and extent of detonation or deflagration of the HE material. In the case of violent detonation, fragmentation of the nuclear material and associated disbursal of solid material would be more prevalent. For the case of an HE burn, release of the nuclear material would be more as an aerosol which would create an internal exposure hazard and perhaps a toxicity problem depending upon the type of fissile material within the pit. (refer to previous discussion on toxicity of plutonium) The burn type of release also creates a higher probability of release to the surrounding environment unless a secondary containment is present and is intact.

Note that in the case of a violent explosive type of reaction, if a secondary containment is present, there is the potential for the explosion to simultaneously breach the containment which would also create a release to the environment, although since the release would in general be disbursal of the fragmented pit, it would likely be more localized than an aerosol-burn release that breached secondary containment.

The population density of the surrounding site
This factor has a direct impact on the gross received dose in that the higher the population density of the area surrounding an accident site, the more individuals that may be exposed and receive a significant radiation dose with either somatic or acute consequential effects.

Weather conditions at the time of and following release

Following a release of radiological materials to the surrounding environment (in the form of a fire, dispersion of aerosols or fine particulate, or a gaseous or liquid vapor), the shape and path of a dispersion plume are heavily influenced by prevailing atmospheric factors. These factors include, wind and wind direction, precipitation and its form (rain, hail, snow, etc.), inversions, thermals, temperature, humidity, and upper atmospheric conditions. Many of these factors influence both the shape, density, and location of the plume and associated deposition of radiological materials that ultimately result in direct exposure to the public or entry into the food chain or surface and subterranean aquifers.

G. Develop activities and alternatives to minimize the risk.

Often times when the risk is unacceptable, a plan must be formulated to minimize the risk. As an example, if an individual works in a facility where a toxic release occurs, an evacuation plan may be developed to minimize the risk to an individual. Similarly, in the design phase of a facility, consideration should be given to the incorporation of passive design features that minimize risk. As an example, the use of natural circulation in the design of the primary loop of a reactor can lead to a walk-away design where the reactor essentially requires no assistance to remain safe following all but the most severe accidents. Another possibility would be the inclusion of an active safety system designed to mitigate the consequences of an accident. An example of such a system would be the emergency core cooling system for a reactor. Here, upon detection of a loss of coolant accident, the system is activated to make-up water lost from the primary coolant break.

In all cases, the process of developing activities and alternatives to minimize risk is reduced to answering questions such as the following. However, these questions are not necessarily complete for a given facility and may not fully represent all considerations. As such, it is the responsibility of each individual to consider all available techniques in developing alternatives to minimize risks. Examples of questions to consider:

- Is the accident avoidable through incorporation of a design or equipment change?
- Is the design/equipment change economically feasible?
- If the answer to either of the above is no, then the following questions must be asked:

- Can the accident initiator frequency be reduced to an acceptable level or eliminated through a systematic process that ensures quality, incorporates redundancy, or provides backup functionality for the initiator in question?
- Can the accident be mitigated through installation of economically feasible SSCs including barriers or active systems designed to reduce the effects of the accident in question?
- Can the consequences be mitigated by minimizing the impacts on the public through remote siting requirements, including such attributes as siting in desolate, remote locations, underground?
- Can the worker or the public be trained to mitigate or minimize exposure to himself/herself through the use of personal protective equipment, procedures, etc.?

The consideration of such alternatives and activities must be addressed and is all the more important in a climate where costs of accidents often exceed the cost of prevention or mitigation or where societal concerns dictate other acceptability standards.

H. Identify the stage of the project in which the risk exists.

Most risk exists in the operational phase of a project, but often times the operational phase may be further broken down into initial or normal startup, normal operations, shutdown, abnormal operations, or even the construction phase. It is notable that the latter is generally not analyzed using probabilistic risk analysis techniques. However, if the facility construction encompasses use of other than normal industrial activities, a construction risk assessment may be desirable. In general, the assessment of each stage or condition may be warranted to identify the stage or condition in which the majority of risk exists. When this is performed, the risk may be quantified for each state or condition with the end result being a weighted average of the stage(s) and condition(s) analyzed according to the anticipated percentage of time expected under each analysis. Conversely, and most commonly, each analysis is performed as a stand alone with results and insights into the dominant contributors for each condition of the plant. This process allows the identification of risk according to the stage or condition of a project or facility. A less rigorous method may also be used such as a FMEA or a similar scoping stage analysis.

References and Suggested Reading

Henley, E. J. and Kumamoto, H., Probabilistic Risk Assessment, The Institute of Electrical and Electronics Engineers, New York, NY, 1992.

Guidelines for Hazard Evaluation Procedures, Center for Chemical Process Safety, American Institute for Chemical Engineers, New York, NY, 1992

Tukey, J. W., Exploratory Data Analysis, Addison-Wesley Publishing Co., Reading, MA, 1977.

Problem Analysis

Section 4

OBJECTIVE

Demonstrate the ability to apply root cause problem analysis methods, determine potential causes of problems, and identify appropriate corrective actions.

1. Define an issues management system, describe its elements, and discuss the importance of issues management to safety, quality, and productivity. **4 - 1**

An issues management system provides concise information regarding the status and importance of facility concerns by categorizing and consolidating these concerns and implementing a mechanism that identifies duplicate efforts and programmatic problems. Its primary objective is the prioritization of issues. Secondly, an issues management program tracks issue status from conception to resolution. The program elements are data gathering, data interpretation, root cause analysis, and corrective action determination.

2. Identify and discuss various problem analysis techniques used within DOE. **4 - 2**

DOE Order 430.1 and OMB Circular A-131 address value engineering and life cycle management of DOE facilities. This process may be applied to risk studies through the use of cost-benefit analysis techniques.

Cost-Benefit Analysis

Cost-benefit analysis seeks to quantify the decrease in risk versus the cost of proposed Structure, Systems and Components (SSCs) additions, modifications or elimination. For example, a facility may be experiencing relatively frequent loss of offsite power and associated blackouts. This represents a potential accident initiator which could lead to undesirable consequences. There are two proposed corrective actions which call for a cost-benefit analysis:

1. add another line to the single radial power line to provide an additional, alternate path for bringing power to the site.

2. install a back-up emergency generator to provide site power when main power to the site is lost.

A cost-benefit analysis would study the impacts that each proposed corrective action would have on lowering the affected accident sequence frequencies. Each proposed corrective action should then result in a decrease in the frequency or consequences for accidents of concern. In this example, the addition of each of these alternatives would result in a lower frequency for site blackout. Each alternative would have an associated cost for equipment installation, operation, maintenance, and removal or decommissioning. A total cost including these and any other known costs is estimated for each alternative. Data for cost estimating is most commonly obtained from current MEANS Cost Estimating Data. The cost-benefit analysis would analyze the ratio of total cost to risk decrease which can be expressed as $/ frequency reduction. Accordingly, the option with the lowest ratio for cost to risk decrease in station blackout would most likely be chosen. This decision would be consistent with value engineering.

Root Cause Problem Analysis

A second problem analysis technique is Root Cause Problem Analysis; the remainder of this section examines this technique.

3. Demonstrate the ability to:

- **explain the elements of DOE problem analysis techniques**
- **determine potential causes of problems using root causes analysis methods**
- **identify corrective actions**

4 - 3

A. Define the terms event, cause, causal factor, direct cause, contributing cause, and root cause.

An **event** is a real-time occurrence such as a pipe break, a valve failure or a loss of power. An event is almost anything that could seriously impact the intended mission of DOE facilities.

A **cause** or **causal factor** is a condition or an event that results in an effect which can be defined as anything that shapes or influences the outcome. A cause may be anything from noise in an instrument channel, a pipe break, an operator error, or a weakness or deficiency in management or administration.

A **causal factor chain** is the cause-and-effect sequence in which a specific action creates a condition that contributes or results in an event. This creates new conditions that, in turn, result in other events.

The **direct cause** is the cause that directly resulted in the event or occurrence. For example, in the case of a leak, the direct cause could have been the failure in the component or equipment that leaked. In the case of a system misalignment, the direct cause could have been operator error in the alignment.

Contributing cause is the cause that contributed to the event but by itself would not have caused the event. An event can have multiple contributing causes. In the case of a leak, the contributing cause could be lack of adequate operator training in leak detection and response which resulted in a more severe event than would have otherwise occurred. In the case of a system misalignment, the contributing cause could be excessive distractions to the operators during the shift which resulted in less than adequate attention to important details during system alignment.

The **root cause** is the cause that, if corrected, would prevent reoccurrence of this and similar events. The root cause not only applies to this event, but it has generic implications to a broad group of possible events. It is the most fundamental aspect of the cause that can logically be identified and corrected. There may be a series of causes that can be identified with one leading to another. This series should be pursued until the fundamental, correctable cause has been identified.

Example:
In the case of a leak, the root cause could be a failure of management to ensure that maintenance is effectively managed and controlled. This cause could have led to the use of improper seal material or missed preventive maintenance on a component which ultimately failed. In the case of a system misalignment, the root cause could be failure in the training program which led to a situation in which operators were not fully familiar with control room procedures and were willing to accept excessive distractions.

B. Discuss the Root Cause Investigation and Reporting Process. List and describe the five steps in the process.

The objective in analyzing and investigating the cause of events is to identify those corrective actions which will be adequate in preventing recurrence and thereby protect the health and safety of the public, the workers, and the environment. The investigation process is used to gain an understanding of the event, its causes, and the corrective actions necessary to prevent recurrence.

Five Phases

Every root cause investigation and reporting process should include five phases. While there may be some overlap between phases, every effort should be made to keep them separate and distinct.

1. Data Collection

   It is important to begin the data collection phase immediately following event identification to ensure that data are not lost. Without compromising safety or recovery, data should be collected during an event. The collected information should consist of:

   - conditions before, during, and after the event
   - personnel involvement and actions taken
   - environmental factors
   - other information relevant to the event.

2. Assessment

   The assessment phase includes analyzing the data in order to identify the causal factors and the causal factor chain.

3. Corrective Actions

   Implementing effective corrective actions for each cause reduces the probability that a problem will recur and improves reliability and safety.

4. Inform

   Management and the personnel involved in an event should receive an explanation on the results of the root cause analysis and its resultant corrective actions. They should also have the opportunity to discuss the results. Management may consider providing any information of interest to other facilities. Also, entering the report into a database system such as ORPS may be part of the inform process.

5. Follow-up

   Follow-up includes determining if corrective action has been effective in resolving problems. An effectiveness review is essential to ensure that corrective actions have been implemented and are preventing recurrence.

C. Discuss the Data Collection phase in detail. List appropriate data gathering techniques and discuss the use of trending and history when conducting a root cause analysis. Discuss the purpose of the interview during this phase.

The basic need in the root cause investigation process is to determine the direct, contributing and root causes in order to identify the corrective actions that will prevent recurrence. The following areas should be considered in determining what information should be gathered:

- activities related to the event
- initial or recurring problems
- equipment or programmatic-type issues associated with the event
- recent administrative program or equipment changes
- physical environment or other influential circumstances.

The identification of problems may at times be as simple as observation. For example, if a facility has operated without a lost time work injury for several months or years and two or more such injuries occur within a relatively short time period, this *could* be an indication of a new problem. This process is generally known as data trending, and it requires careful attention to detail by both managers and operators. A more thorough treatment of the statistics used in support of data trending analysis can be found in Section 1.

Three methods are available for gathering information: conducting interviews or collecting statements from individuals involved in the event, interviewing other personnel who have performed the job in the past, and reviewing records and relevant documents. When interviewing individuals, consider using a walk-through as part of the interview. Records to review may include operating logs, correspondence, maintenance records, inspection/surveillance records, and procedures and instructions. A complete list of

recommended records and documents can be found in DOE-NE-STD-1004-92.

The most important point to remember when conducting interviews is to keep them fact finding rather than fault finding. Prepare your interview questions in advance to ensure that all necessary information is obtained, but questions can be modified or amplified depending upon responses to the questions. Interviews are the preferred method, and they should be conducted with the people who are most familiar with the problem.

D. Discuss the Assessment phase in detail. List the basic steps in analyzing and determining the events and causal factor chain.

The primary goal of the assessment phase is to determine the causal factor chain. The first step is problem identification. It is important to remember that the event may not be the problem.

Example:
The actuation of a protective system constitutes the event but is not the real problem; the unwanted, unplanned condition or action that resulted in actuation is the problem to be solved. Dust in the air actuates a false fire alarm. In this case, the event is the actuation of an engineered safety feature. The smoke detector and alarm functioned as intended; the problem to be solved is the dust in the air – not the false fire alarm.

The second step is determination of the problem's significance. This step is important because the level of effort for the remainder of the assessment is dependent upon the problem's potential consequences. The significance can be assessed by questioning the severity of the consequences, the likelihood of recurrence, the severity of the consequences should the event happen again, the presence of poor attitudes, a safety culture problem, or a widespread program deficiency.

The third step is to identify the causes that immediately preceded and surrounded the problem. The causes can be conditions or actions. The objective is the identification of the root cause. Cause identification should focus on programmatic and system deficiencies and avoid simple excuses such as blaming the employee. It is helpful

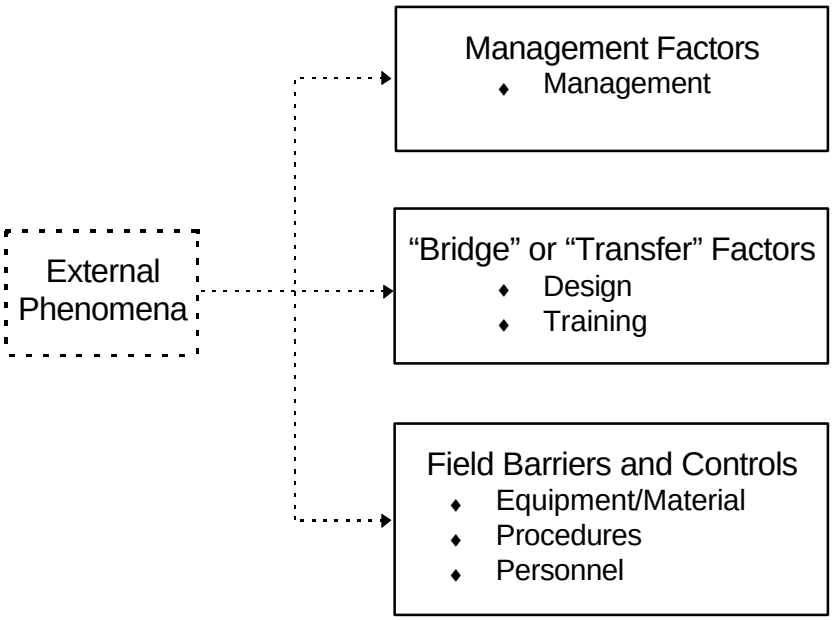
to keep in mind that the root cause is an explanation of why the direct cause occurred; it is not a repetition of the direct cause. If ORPS cause categorization is used, the cause description is not a repetition of the cause category description; it is a description specific to the occurrence.

Cause categorization can be performed in this step. The ORPS cause code categories were carefully selected with the intent of addressing all problems that could arise in conducting DOE operations. Consider this brief explanation of the ORPS cause codes. The elements necessary to perform any task are equipment/material, procedures, and personnel. Design determines the quality and effectiveness of equipment while training serves the same purposes for personnel. Since these five elements must be managed, management is also a necessary element. Whenever an event occurs, one of these six program elements was inadequate to prevent the event. The seventh element included in the DOE cause categorization is the “external phenomenon” event. Events whose cause is attributed to this category include only those events that are beyond operational control. (ORPS also provides for radiological/hazardous material problem as an additional cause categorization.)

These seven causal factors can be associated in a logical causal factor chain as shown in Figure 4.1. A direct, contributing, or root cause can occur any place in the causal factor chain. A root cause can be an operator error while a management problem can be a direct cause.

Causal Factor Categories Associated in a Logical Chain

Figure 4.1



Within the seven causal factor categories, there are a total of 32 cause subcategories. The direct cause, contributing causes, and root causes are all selected from these subcategories. As an example, there are six subcategories associated with equipment/material causal factors including:

- Defective or failed part
- Defective or failed material
- Defective weld, braze, or soldered joint
- Error by Manufacturer in shipping or marking
- Electrical or instrument noise
- Contamination

The above and other subcategories categorized by the seven causal categories are listed on the equipment/material worksheet contained in DOE-NE-STD-1004-92. (The student is referred to the standard for further discussion and worksheet use.) Following a root cause investigation, the seven worksheets containing the 32 causal factor subcategories may be used by the analyst to assist in categorizing the various contributing, direct, and root causes of the accident or occurrence for use within the ORPS database.

In summary, the goal of performing the above process is to identify and classify the reasons why the direct and contributing causes identified in the preceding step existed. If these are addressed, identification of the root cause may be determined. The identification of the root cause is the stopping point in the assessment of causal factors. It is the place where, with appropriate corrective action, the problem will be eliminated

and not recur. The worksheets contained in DOE-NE-STD-1004-92 are designed as an aid to assist the analyst with specific categories and subcategories into which all accidents or occurrence direct, contributing, and root causes may be classified for documentation in the ORPS database.

E. Discuss and describe the most common root cause analysis methods. List the advantages and disadvantages of each method. Provide examples or explain the methodology in conducting each method.

- **Events and Causal Factor Analysis**
- **Change Analysis**
- **Barrier Analysis**
- **Management Oversight and Risk Tree (MORT) Analysis**
- **Human Performance Evaluation**
- **Kepner-Tregoe Problem Solving and Decision Making**

A number of methods for performing root cause analysis are available. Many of these methods are specialized and apply to specific situations or objectives. Most have their own cause categorizations, but all are very effective when used within the scope for which they were designed. The most common methods are:

- Events and Causal Factor Analysis
- Change Analysis
- Barrier Analysis
- Management Oversight and Risk Tree (MORT) Analysis
- Human Performance Evaluation
- Kepner-Tregoe Problem Solving and Decision Making.

A summary of the most common root cause methods, when it is appropriate to use each method, and the advantages and disadvantages of each are provided in Table 4.1 and Figure 4.2. The extent to which these methods are used and the level of analytical effort spent on root cause analysis should be commensurate with the significance of the event. In any case, the depth of analysis should be adequate to explain why the event happened, determine how to prevent reoccurrence, and assign responsibility for corrective actions.

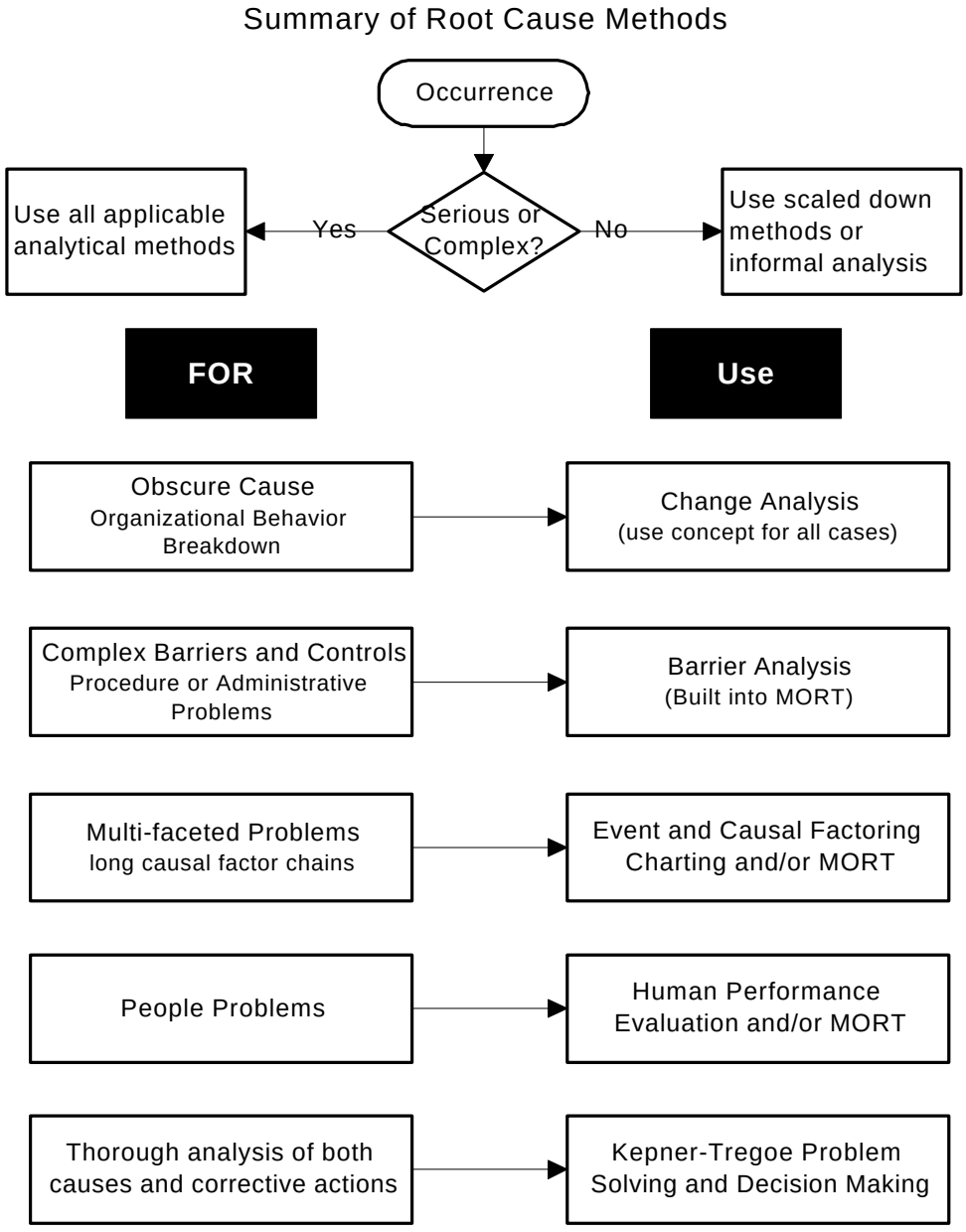
Summary of Root Cause Methods

Table 4.1

Method	When to use	Advantages	Disadvantages
Event and Causal Factor Analysis	Multi-faceted problems with long or complex causal factor chain	Provides visual display of analysis process. Identifies probable contributors to the conditions	Time-consuming and requires familiarity with process to be effective
Change Analysis	Cause is obscure. Especially useful in evaluating equipment failures	Simple 6-step process	Limited value because of the danger of accepting wrong, "obvious" answer
Barrier Analysis	Identify barrier and equipment failures and procedural or administrative problems	Provides systematic approach	Requires familiarity with process to be effective
MORT and mini-MORT	Shortage of experts to ask the right questions and whenever the problem is a recurring one. Helpful in solving programmatic problems	Can be used with limited prior training. Provides a list of questions for specific control and management factors	May only identify area of cause, not specific causes
Human Performance Evaluations (HPE)	People identified as being involved in the problem cause	Thorough analysis	None if process is closely followed
Kepner-Tregoe	Use for major concerns where all aspects need thorough analysis	Highly structured approach focuses on all aspects of the event and problem resolution	More comprehensive than may be needed

A high-level effort includes use and documentation of formal root cause analysis to identify the upstream factors and the program deficiencies. Both Events and Causal Factor Analysis and MORT could be used together in an extensive investigation of the causal factor chain. An intermediate level might be simple Barrier, Change, or mini-MORT analysis. A low-level effort may only include gathering information and drawing conclusions without documenting the use of any formal analytical method. However, a thorough knowledge and understanding of root cause analytical methods is essential to conducting the correct type of investigation in order to obtain meaningful conclusions.

Figure 4.2



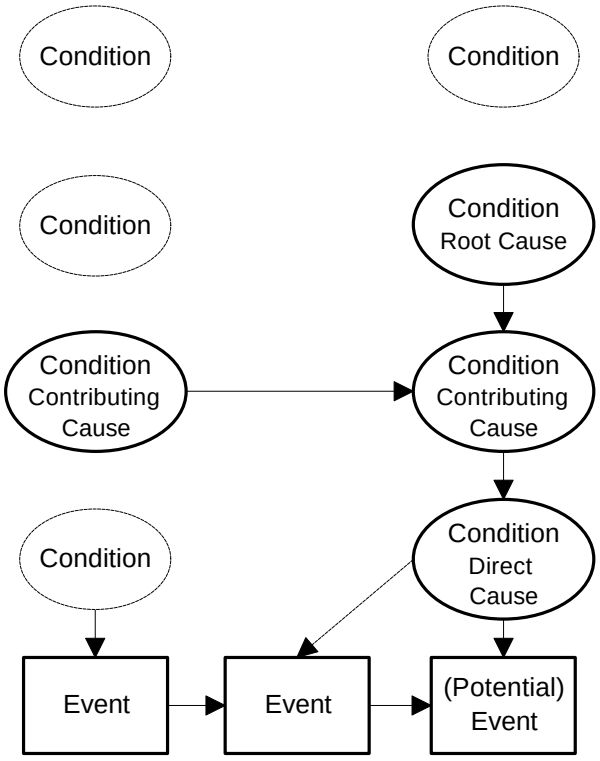
Events and Causal Factor Analysis

Events and Causal Factor Analysis is used for multi-faceted problems or long, complex causal factor chains. The resulting chart is a cause and effect diagram that describes the time sequence of a series of tasks and/or actions and the surrounding conditions leading to an event. The event line is a time sequence of actions or happenings while the conditions are anything that shapes the outcome and ranges from physical conditions to attitude or safety culture. The events and conditions as given on the chart describe a

causal factor chain. The direct, root, and contributing cause relationships in the causal factor chain are shown in Figure 4.3.

Figure 4.3

Causal Factor Relationships



The following definitions apply to Figure 4.3

The sequence of real-time happenings or actions

Any as-found or existing state that influences the outcome of a particular task, process, or operations

Conditions that may exist but are not identified

This diagram is a graphical display of what is known. Since all conditions are a result of prior actions, the diagram identifies what questions to ask in order to follow the path to the source or root cause. In real life, the causal factor chain will usually be complex with many branches. In such cases, a diagram will be necessary to understand what happened and why. The cause and effect block diagram offers these advantages:

- It provides a means for organizing the occurrence data.

- Since it provides the investigator with a concise summary of what is known and what is unknown, it serves as a guide to direct the course of the investigation.
- It results in a detailed display of the sequence of facts, conditions, and activities.
- It assists in organization of report data and provides a picture format for briefing management.

Change Analysis

Change Analysis is used when the problem is obscure. It is a systematic process that is generally used for a single event and focuses on elements that have changed. It analyzes the deviation between what is expected and what actually happened. The evaluator essentially asks what differences occurred to make the outcome of this task or activity different from all the other times this task or activity was successfully completed. Figure 4.4 shows the steps in the Change Analysis method.

Change Analysis Steps

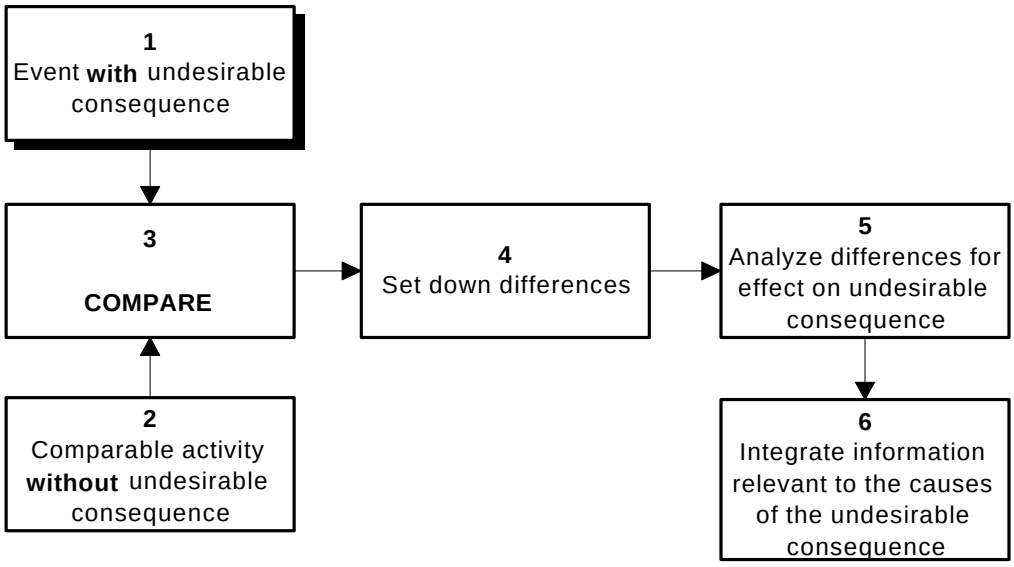


Figure 4.4

This technique consists of asking the questions – What, When, Where, Who, and How. Answering these questions should provide direction toward answering the root cause determination question – Why. Change analysis is a good technique to use whenever the causes of the condition are obscure, you do not know where to start, or you suspect a change may have contributed to the condition. On

the other hand, this technique is not thorough enough to determine all the causes of more complex conditions.

A Change Analysis Worksheet is an excellent tool to use while asking questions, noting differences or changes against the ideal situation, and recording the effects while in the process of determining the root cause. A worksheet is provided as Table 4.2.

Table 4.2

Change Analysis Work Sheet

Change Factor	Difference or Change	Effect	Questions to Answer
WHAT Conditions, event, activity, equipment			
WHEN occurred, identified, plant status, schedule			
WHERE physical location, environmental conditions			
HOW work practice, omission, extraneous action, out of sequence procedure			
WHO personnel involved, training, qualification, supervision			

Barrier Analysis

Barrier Analysis is a systematic process used to identify physical, administrative, and procedural barriers or controls that should have prevented the event. This technique should be used to determine why these barriers or controls failed and what is needed to prevent recurrence.

The DOE Root Cause Analysis Standard defines a barrier using MORT terminology. It is something that separates an affected component from an undesirable condition or situation. Figure 4.5 provides an example of a barrier analysis. Several questions listed in DOE-NE-STD-1004-92 can be used in determining what barrier failed and led to the event.

Barrier Analysis Example for a Clean Relay Contact

Work Task: Clean Relay Contact
Occurrence: Relay Trip

Sequence of Events:

System Tagout Requested → Warning Tag Hung → Maintenance electricians given assignment → Electricians follow procedure → **REACTOR TRIP**

Barrier Analysis:

Start of work process → Tagout process Step 1 → Tagout process Step 2 → Communication Process Interface → Procedure → Training → **Occurrence**

MWR requests de-energizing two panels so relays can be cleaned. Operations will only allow one panel at a time to be tagged out. Electrical foreman told and agrees.	Tag hung on P689 - only P690 is still energized	Electricians given MWR to work, which references a Maint. procedure, but not told of change in scope by foreman.	Electricians go to P690 and begin procedure. Procedure has no step to verify dead power supply before starting. They open first relay and plant trips.	Electricians never trained to always check power supply prior to working on electrical equipment.
Barrier Holds	**Barrier Holds**	**Barrier Fails**	**Barrier Fails**	**Barrier Fails**

Figure 4.5

Management Oversight and Risk Tree (MORT)

MORT and mini-MORT is used to prevent oversight in the identification of causal factors. It lists on the left side of the tree specific factors relating to the occurrence; and on the right side of the tree, it lists the management deficiencies that permit specific factors to exist. The management factors all support each of the specific barrier/control factors. Included is a set of questions to be asked for each of the factors on the tree. As such, it is useful in preventing oversight and ensuring that all potential causal factors are considered. It is especially useful when there is a shortage of experts to ask the right questions.

However, because each of the management factors may apply to the specific barrier/control factors, the direct linkage or relationship is not shown but is left up to the analyst. For this reason, Events and Causal Factor Analysis and MORT should be used together for serious occurrences: one to show the relations, the other to prevent oversight.

Human Performance Evaluation

Human Performance Evaluation is used to identify factors that influence task performance. It is most frequently used for man-machine interface studies. Its focus is on operability and work environment rather than on training operators to compensate for bad conditions. Also, human performance evaluation may be used for most events since many conditions and situations leading to an event ultimately result from some task performance problem such as planning, scheduling, task assignment analysis, maintenance, and inspections. Training in ergonomics and human factors is needed to perform adequate human performance evaluations, especially in man-machine interface situations.

Kepner-Tregoe Problem Solving and Decision Making

Kepner-Tregoe is used when a comprehensive analysis is needed for all phases of the occurrence investigation process. Its strength lies in providing an efficient, systematic framework for gathering, organizing, and evaluating information and consists of four basic steps:

1. Situation appraisal to identify concerns, set priorities, and plan the next steps.
2. Problem analysis to precisely describe the problem, identify and evaluate the causes, and confirm the true case.
3. Decision analysis to clarify purpose, evaluate alternatives, assess the risks of each option, and make a final decision.
4. Potential problem analysis to identify safety degradation that might be introduced by the corrective action, identify the likely causes of those problems, take preventative action, and plan contingent action. This final step provides assurance that the safety of no other systems is degraded by changes introduced by the proposed corrective actions.

These four steps cover all phases of the occurrence investigation process and thus, Kepner-Tregoe can be used for more than causal factor analysis.

F. Explain and apply problem analysis techniques to identify *potential* problems and/or prevent problems.

The identification of problems may at times be as simple as observation. For example, if a facility has operated without a lost time work injury for several months or years and two or more such injuries occur within a relatively short time period, this*could* be an indication of a new problem. This process is generally known as data trending, and it requires careful attention to detail by both managers and operators. A more thorough treatment of the statistics used in support of data trending analysis can be found in Section 1.

This concept may be extended into prevention and identification of potential problems through observation of performance trends (such as maintenance induced equipment failures) whose function may or may not be safety related and extending this observation using the "what if" mode to anticipate similar trends for safety related SSCs having similar types of equipment.

G. Define the term corrective action and discuss the elements of an effective corrective actions program.

A corrective action is that action which is identified to remedy the problem, and when completed, will prevent recurrence.

Effective Corrective Action Program

The root cause analysis enables improvement of reliability and safety by selecting and implementing effective corrective actions. Effective corrective action programs include:

- Management emphasis on the identification and correction of problems that can affect human and equipment performance, including assigning qualified personnel to effectively evaluate equipment/human performance problems, implementing corrective actions, and following up to verify that corrective actions are effective.
- Development of administrative procedures that describe the process, identify resources, and assign responsibility.

- Development of a working environment that requires accountability for correction of impediments to error-free task performance and reliable equipment performance.
- Development of a working environment that encourages voluntary reporting of deficiencies, errors, or omissions.
- Training programs for individuals in root-cause analysis.
- Training of personnel and managers to recognize and report occurrences, including early identification of significant and generic problems.
- Development of programs to ensure prompt investigation following an event or identification of declining trends in performance to determine root causes and corrective actions.
- Adoption of a classification and trending mechanism that identifies those factors that continue to cause problems and generic implications.

Corrective Action Implementation

The first step in implementing immediate or long-term corrective actions is to identify the corrective action for each cause and then apply the following criteria to the corrective action to ensure it is viable. If the corrective action is not viable after asking the questions, the solution must be reevaluated.

1. Will the corrective action prevent recurrence?
2. Is the corrective action feasible?
3. Does the corrective action allow meeting primary objectives or mission?
4. Does the corrective action introduce new risks? Are the assumed risks clearly stated? (The safety of other systems must not be degraded by the proposed corrective action.)

A systems approach, such as Kepner-Tregoe, should be used in determining appropriate corrective actions. It should consider not only the impact they will have on preventing recurrence, but also the potential that the corrective actions may actually degrade some other aspect of safety. Also, the impact of the corrective actions on other facilities and their operations should be considered. The proposed immediate or long-term corrective actions must be compatible with facility commitments and other obligations. In addition, those affected by or responsible for any part of the corrective actions should be

involved in the process. Proposed immediate or long-term corrective actions should be:

- reviewed to ensure the above criteria have been met
- prioritized based on importance
- scheduled and a change in priority or schedule should be approved by management
- entered into a commitment tracking system
- implemented in a timely manner.

A complete corrective action program should be based, not only on specific causes of events, but also on items such as lessons learned from other facilities, appraisals, and employee suggestions.

A successful corrective action program requires management that is involved at the appropriate level and is willing to take responsibility and allocate adequate resources for corrective actions.

H. Given the data for an event/occurrence, determine the root cause, direct cause and contributing causes and develop corrective actions. Discuss how the problem might have been avoided.

An experiment high-temperature alarm occurred during reactor startup. (Root Cause analysis done with change analysis, mini-MORT or Cause and Effects are adequate for this investigation.) It was revealed that

- The cooling gas was hooked to the wrong cylinder.
- The operator had followed the startup procedure to verify correct hook up.
- The procedure was not sufficiently detailed to ensure adequate verification (the procedure did not state that the operator was to verify the correct hookup, only to verify that correct gas mixture in the cylinder).
- The cylinders had been moved by maintenance personnel to facilitate other noncylinder work in the area and had been returned to the wrong position in the rack (management did not want the cylinders moved by maintenance, but had not implemented any controls).
- The cylinders were not color coded.

This was classified as an off-normal occurrence related to nuclear safety. The problem was inadequate cooling and the resulting high temperature in the experiment loop. The direct cause was not verifying correct hookup because of inadequate startup procedures (Cause Code 2A, Procedure Problem, Defective or Inadequate Procedure.) Contributing causes were maintenance personnel returning the cylinder to the wrong position (Case Code 3B, Personnel, Inadequate Attention to Detail), and the identical leads and colors of cylinders with different contents (Cause Code 4A, Design, Inadequate Man-Machine Interface.) The root cause was determined to be the prevailing attitudes and culture that contributed to the maintenance errors and poor design (Cause Code 6E, Management, Policy not Adequately Defined, Disseminated or Enforced). In this case, personnel error is not a valid cause because the operator had not been trained to this requirement and should not have been expected to take the extra precautions.

Note that in this case, as a minimum, corrective action should include review and revision where appropriate of other procedures and training operators to the new procedures. Further corrective action would include installation of fittings that make it impossible to hook up the wrong cylinder, a review of other hookups within the facility to correct similar problems, and the use of human factors in configuration design and control.

I. Compare and contrast immediate, short-term, and long-term corrective actions taken and recommended as the result of a root cause analysis of an event or occurrence.

From the viewpoint of a Facility Manager, immediate, short-term and long-term corrective actions have the following perspective.

Immediate corrective actions are generally taken to avoid death, injury, damage, or uncontrolled environmental hazards. They are also taken to avoid the potential for these events to occur. If an event has already occurred, immediate actions may be taken to prevent recurrence or to mitigate or minimize potential consequences. These actions may be inconsistent with the facility mission, but they may be warranted given the seriousness or potential consequences of an event. In effect, immediate corrective actions are those actions which may be taken to place a facility in a safe condition given an expectation or an occurrence of a serious event.

Short-term corrective actions are taken to minimize risk following an event or in anticipation of an event. The corrective actions taken are not necessarily inconsistent with the longer term facility mission, but they may be necessary in order to minimize or avoid the effects of a serious event. These actions may or may not follow an initial investigation into the nearly missed or unusual event and are generally designed to provide temporary relief from occurrences or near occurrences so as to permit continued operation or restart of a facility in the short term.

Long-term corrective actions are taken following a thorough investigation into the root cause for a nearly missed or unusual event. These actions are designed to address the root cause of the near-miss or unusual event and may reinforce immediate or short-term action previously taken. They are almost always consistent with the long term facility mission.

In effect, immediate, short-term and long-term corrective actions reflect the maturity of root cause knowledge held by the individuals implementing the corrective actions. As additional analysis is performed on the root cause for a given event, the corrective action path taken is more likely to move toward elimination of the root cause, thereby allowing for effective long-term actions.

J. Observe a contractor problem analysis and critique their results.

As part of an exercise for this section, observe a problem analysis and discuss your critique of the results with your supervisor as part of completing this competency.

K. Participate in at least one contractor or Department problem analysis and critique its results.

As part of an exercise for this section, observe a second problem analysis and discuss your critique of the results with your supervisor as part of completing this competency.

L. Conduct an interview representative of one which would be conducted during an occurrence investigation.

As part of an exercise for this section, simulate an occurrence investigation interview for an occurrence which has recently happened at your facility. Have your supervisor observe the interview and discuss your performance.

M. Using contractor training procedures, applicable DOE Orders, and DOE Standard 1070-94, Guidelines for Evaluation of Nuclear Facility Training Programs, select three elements of the contractor training program and assess them for compliance and adequacy.

As part of an exercise for this section, access a copy of contractor training procedures and the referenced orders, standards and guidelines. Assess three elements of the contractor training program for compliance and adequacy. Review your analysis with your supervisor as part of completing this competency.

References and Suggested Reading

References and Suggested Reading

Department of Energy, Root Cause Guidance Document (DOE-NE-STD-1004-92), DOE, 1992.

Hazard Analysis

Section 5

OBJECTIVE

Demonstrate knowledge of hazard analysis techniques applicable to systems, processes/operations, and

1. Demonstrate knowledge of hazard analysis techniques applicable to systems, processes/operations, and jobs.

5 - 1

A. For a given operation, identify and perform appropriate job safety analysis techniques, and make necessary recommendations.

The definition of hazard evaluation as defined by the American Institute of Chemical Engineers (AICHE) is the following:

> The analysis of the significance of hazardous situations associated with a process or activity. This analysis uses qualitative techniques to pinpoint weaknesses in the design and operation of facilities that could lead to accidents.

The process of assessing project risks to identify critical systems, subsystems, and other factors requiring focused work and resolution is summarized by the questions:

- What could go wrong?
- How likely is it?
- What are the consequences?

How the process is applied consists essentially of the following:

- Establish the scope of the study. (The scope will include earthquakes, tornadoes, flooding, internal failures, sabotage, study boundaries, etc.)
- Identify the hazards.
- Identify the parts of the process or system that give rise to the hazards identified.
- Classify hazards into Category 1, 2, and 3 according to hazard consequences.

- Identify all active systems, barriers, components, and other passive design features designed to address or mitigate Category 1 and 2 (and in some cases Category 3) hazards.
- Prepare and document a Preliminary Hazards Analysis (PHA) to further qualify accident sequences (Optional). Another equivalent technique may be used.

Generally, for a hazard evaluation, qualitative and lesser quantitative techniques are used to arrive at a hazard determination as defined by the following hazard category levels:

- Category 1: Hazards show significant offsite consequences
- Category 2: Hazards show significant onsite consequences
- Category 3: Hazards show only localized consequences.

The end result of the hazard evaluation without a PHA is the identification of those hazards that have adverse impacts on the population or the environment as well as adverse economic impacts such as a negative image or loss of market share. The PHA takes the process one step further and identifies structures, systems, components, administrative controls, and any other factors that are required to maintain qualitatively acceptable risk levels.

There are various hazard evaluation techniques which may be employed to identify and define hazards and in some cases further identify an accident sequence. The following is a list of techniques which may be used for hazard analysis:

- Preliminary Hazards Analysis (PHA)
- Failure Modes and Effects Analysis (FMEA)
- Failure Modes and Effects Criticality Analysis (FMECA)
- Hazard and Operability Analysis (HAZOP)
- Event Tree Analysis (FTA)
- Fault Tree Analysis (ETA)
- Energy Trace and Barrier Analysis
- Operating and Support Hazard Analysis
- System/subsystem Hazard Analysis
- Hazard Evaluation
- Human Reliability Analysis (HRA).

The more commonly used techniques are discussed in further detail under Objective 1.B. All techniques seek to identify the hazards that

could be a source of risk. Some techniques further classify the hazards, and still others further define accident mitigation or prevention functions. Examples of hazards are the following:

- Combustible Material
- High Pressure Piping
- Caustic/Corrosive Chemicals
- Chemical Solutions
- Radionuclide Inventory
- Potential Energy (e.g. Dams, Objects suspended at high height, etc.)
- Biological Hazards
- Toxic Hazards
- Kinetic Energy (e.g. Rotating Machinery, Rivers, etc.)
- Electrical Energy
- High Temperatures
- Cryogenics.

Ultimately, based upon a hazard analysis of a facility or process, hazards are identified which have unacceptable risk. From this analysis and from further analysis, mitigating or preventive measures may be identified to address the risk. As a result, recommendations may be made and incorporated into design or subsequent facility modifications to reduce risk to acceptable levels and within acceptable costs.

It is important to understand that the hazard evaluation process (at best) generally provides a relative, non-absolute evaluation or ranking of risk issues. In fact, some techniques may provide not ranking information at all. This in part is one reason for the necessity of continuous reevaluation throughout facility life cycle as issues and new hazards or accident types are introduced, discovered, or existing ones become better defined or understood.

B. Discuss the need for, and the selection and performance of the applicable qualitative techniques of system safety analysis, such as:

- **Preliminary Hazard Analysis (PHA)**
- **Failure Modes and Effects Analysis (FMEA)**
- **Failure Modes and Effects Criticality Analysis (FMECA)**
- **Fault Tree Analysis (FTA)**
- **Event Tree Analysis (ETA)**
- **Fault/Event Tree Analysis**
- **Hazard and Operability Analysis (HAZOP)**
- **Energy Trace and Barrier Analysis**
- **Human Reliability Analysis (HRA)**
- **Operating and Support Hazard Analysis**
- **Hazard Evaluation**

Preliminary Hazard Analysis (PHA)

PHA techniques are frequently used when it is desired to include the analysis of event sequences that transform hazards into accidents. Additionally, PHA considers corrective measures and consequences of an accident. Table 5.1 represents the preliminary hazard analysis format for two hazardous situations:

1. hydrochloric acid is introduced into water
2. high temperature chloride-water mixture introduced into stainless steel tank.

Table 5.1

Preliminary Hazard Analysis Example Format

Hazardous Element	Exothermic Reaction	Corrosion/Pitting
Triggering Event 1	Hydrochloric acid introduced into water	Contents of stainless steel tank contaminated with high temperature chloride-water mixture
Hazardous Condition	Potential to initiate strong acid ionization reaction	Chloride pitting inside stainless steel tank
Triggering Event 2	Container outside of hood	Operating pressure of tank exceeded
Potential Accident	Explosion, acid dispersal/splash	Stainless steel tank rupture
Effect	Personnel injury and acid burns; Damage to surrounding structures	Personnel injury from explosive energy and burns; Damage to surrounding structures
Corrective Measures	Add water into hydrochloric acid; disseminate lessons learned on above hazards; perform reactive chemistry inside hoods; wear personal protective equipment (PPE)	Use mild steel or a lined tank; eliminate chlorides; locate tank at a suitable distance from personnel and equipment

Figure 5.1 has been adapted from “Guidelines for Hazard Evaluation Procedures,” (see References), and summarizes the process of hazard identification, hazard evaluation, and risk analysis. Figure 5.1 is located at the end of this section on page 5-13.

In general, PHAs attempt to identify the system events and hardware that can lead to hazards. This step is normally performed during the initial design phase so that insights may be incorporated into designs.

Failure Modes and Effects Analysis (FMEA)

The FMEA process is an inductive logic approach to the identification of all possible failure modes and their effects for all equipment on a component-by-component basis. This process identifies single failure modes only in accordance with the requirements of IEEE 279-1971, 10 CFR Appendix K, and Regulatory Guide 1.7. A FMEA is generally

much more detailed than a fault tree analysis since all failure modes are considered rather than only considering dominant ones as is typical in a fault tree analysis. As an example, the failure modes for a relay are presented in Table 5.2.

Table 5.2

Sample Relay Failure Modes

◆ contacts stuck open
◆ contacts stuck closed
◆ contacts slow to open
◆ contacts slow to close
◆ contacts bent, no contact
◆ contact short circuit
  ◦ to ground
  ◦ to supply
  ◦ between contacts
  ◦ to signal lines
◆ contacts arcing, generating noise
◆ contacts oxidized, current low
	◆ contact resistance
	  ◦ high
	  ◦ low
	◆ coil overheating/breakdown
	◆ coil open circuit
	◆ coil short circuit
	  ◦ to supply
	  ◦ to contacts
	  ◦ to itself
	◆ contact - coil armature arm mechanically stuck
	◆ relay overmagnetized or excessive hysterisis

As a consequence of the analysis, a qualitative, systematic list of equipment, failure modes and associated effects is developed. The worst case consequences of a single failure are also given with recommendations for improving safety for individual failures. The end result is the generation of recommendations for increasing equipment reliability and thus improving safety.

Failure Modes and Effects Criticality Analysis (FMECA)

The use of the word “criticality” in this technique refers to the assignment of a severity attribute to a component failure in an FMEA. This technique may be used within a FMEA or another analysis to extend the analysis and include or rank failure severity. Hence, where this method is employed in FMEA as well as other hazard evaluation techniques, it merely attempts to assign a severity attribute to an individual or conservatively to a similar group of failures in the interest of bounding risk. This process may be used to scope hazard severity and assist in the prioritization of hazards and accidents.

Fault Tree Analysis (FTA)

The FTA process is a deductive technique used to identify combinations of equipment failures, other structures or phenomenological events, or external event failures that can result in the transformation of a hazard into an event of concern or an accident. The results are quantitative in nature which allows relative risk ranking for individual or combinations of failures that may lead to the event of concern and generally unacceptable risk. This technique was addressed in Section 2.

Event Tree Analysis (ETA)

An event tree analysis considers the responses of safety systems, operators, and any related phenomenological events to an initiating event and determines the various possible outcomes from the accident. The results of an event tree analysis are sequences of events defined by successes or failures of individual events leading to accident sequences. Event tree analysis is best suited for analysis of complex facilities where there are multiple preventive or mitigative barriers along with systems or emergency procedures designed to respond to specific initiating events. The structure of event trees was addressed in Section 2.

Fault/Event Tree Analysis

A fault tree/event tree analysis is generally performed to develop a more detailed, quantified picture of facility or integrated systems risk where there are likely to be a number of support systems whose failure could collectively impact mitigative or preventive structures, systems, components, or barriers. The process involves development of event trees that model accident progression for all sequences of interest. This is accomplished by creating an event tree for a single or a group of similar hazards/accidents where the response of preventive or mitigative SSCs would be expected to be the same. For each event tree top requiring more than just a simple yes/no quantification, a fault tree is usually developed that includes interdependencies between SSCs and:

- the initiating hazard or event
- other event tree top SSCs
- the accident progression environment.

An example of the first dependency would be the loss of a common (normal) cooling water supply to a normal cooling water system where the water supply is also the normal supply for another separate core injection system. In this instance, if the water supply were to be lost or became non-functional, the loss of normal cooling water would act as an initiator while the loss of the core injection system would simultaneously be defeated. For the second dependency, if the system fails to provide power, all subsequent system components requiring electric power downstream from the failure could be non-functional. This example may be limited to failure of equipment fed from a common breaker, panel, etc., or it could be as involved as a site/facility blackout depending on the cause of the initial loss, i.e., it could be a failed breaker, a bus, a transformer, or loss of off-site power. For the third example, an internal flooding incident where a pipe break from a cooling system could spray or flood out surrounding equipment and result in their inability to perform as designed.

Upon completion of the development of all fault trees, the sequences are written in terms of a Boolean equation that combines the combinations of successes and failures to represent a single event tree sequence. When this is completed for all sequences of all accident types, the resulting sequences are solved using a computer; and numerical results representing minimal cut set failures are calculated. A running total of all unique cut sets is calculated to determine the total combined sequence risk frequency. Further studies may be performed on the results to determine individual (fractional) sequence, system, component, etc. contribution to risk.

Hazard and Operability Analysis (HAZOP)

This technique was developed to identify and evaluate safety hazards in a process plant and to identify operability problems which, although not necessarily hazardous, may result in the inability of a plant or process to achieve design productivity. To perform a HAZOP analysis, original and current (if modified) design and operating information must be available. Consequently, HAZOP analyses are most commonly performed immediately following the detailed design phase. Similar to the PHA, an interdisciplinary team uses a creative, systematic approach that identifies hazard and operability problems that may result from deviations in process design intent.

The purpose of the HAZOP analysis is to systematically review a process or operation to determine whether process deviations can lead to undesirable consequences. The process may be used for either batch or continuous processes as well as for evaluation of written procedures. A simple example of a batch process would be the titration of one substance into a mixing container while for a continuous process, the oil cracking process, would contain several such examples. Where the team discovers that there is inadequate protection against a given process deviation, a recommendation is made to reduce risk.

Using the HAZOP process, the team is likely to:

- identify both hazards and operating problems
- make recommendations for design, administrative, or procedural changes that may improve the system as well as recommendations for further study.

Energy Trace and Barrier Analysis

The energy trace and barrier analysis method is a systematic process used to identify physical, administrative, and procedural barriers or controls that should have prevented the occurrence. This technique should be used to determine why these barriers or controls failed and what is needed to prevent recurrence. A sample Barrier Analysis is found in Section 4.

Human Reliability Analysis (HRA)

Human Reliability Analysis is the systematic process of evaluation of human performance and associated impacts on SSCs for a facility. The process is generally applied to analyze the factors that influence the performance of operators, supervisors, maintenance personnel, and any other personnel that may influence accident sequence progression and severity. HRA techniques are generally used to analyze errors of omission such as failure to follow a specified procedure rather than errors of commission which are difficult to predict and/or may actually be outright acts of sabotage. The process identifies potential human errors and their effects including underlying causes if possible.

HRA is generally an input into other types of analysis such as fault tree/event tree. It is used to quantify specified human performance such as the use of a procedure that directs the operator/supervisor to

initiate emergency core cooling upon initiation of a large loss of cooling accident. It may also be used to perform isolated analysis of individual operating or maintenance procedures in order to better understand the larger contributors to the risk associated with performance of a specified operation or procedure. The process lists the errors likely to be encountered during performance of a given procedure, factors influencing performance, and those proposed modifications likely to reduce errors during performance. The analysis also identifies those system interfaces that are affected by such errors.

Operating and Support Hazard Analysis

This process is a subset of the hazard evaluation process discussed in the next paragraph.

Hazard Evaluation (including system and subsystem)

The hazard evaluation process has been performed by the chemical process industry in excess of 35 years. Historically, the process has been known by several different names including process hazard analysis, process hazard review, process safety review, process risk review, predictive hazard evaluation, hazard assessment, process risk survey, and hazard study.

To perform a hazard evaluation, all hazards associated with a facility or process to be studied must first be identified. Upon completion of this phase, the hazard evaluation process focuses on the potential causes and consequences associated with those hazards that are created from episodic or catastrophic events.

An example would be an accidental release of gas from a storage cylinder. This is opposed to those hazards that routinely exist at a facility or may occasionally occur. An example of these would be slips from ladders, injury from the use of industrial tools such as drills or saws, continuous releases of exhaust gases from internal combustion engines, or intentional process exhaust from a stack.

The latter hazards are normally addressed by design considerations and good housekeeping practices. Hazard evaluation however attempts to focus on the facility internal SSC failures, external events, and human influenced performance events that may lead to catastrophic releases of energy, toxic, radiological, and biologically harmful materials that may harm the surrounding environment.

Summary

Hazard evaluations normally involve the combined efforts of a multi-disciplinary team that combines the experience, judgment, and expertise to address the diverse range of problems and recommend solutions or further studies. Where information is inadequate and further study is warranted, techniques involving more quantitative risk assessment measures are often employed to give the team additional information needed for decision making. For further assistance in the use of the hazard evaluations process, the student is to refer to the worked examples in the Second Edition of Hazard Evaluation Procedures.

C. Describe the bases upon which to judge the adequacy of a hazard evaluation.

The bases for judging adequacy of a hazard evaluation includes the consideration of a number of factors. These factors are discussed individually in the following subsections and typically consist of:

Thoroughness of hazard identification

The thoroughness of any hazard identification process is rooted in a systematic approach to the identification of all potential site/facility hazards. Typically this process involves two key tasks; identification of specific undesirable consequences, and, identification of material, system, process, and plant characteristics that could produce those consequences.

Identification of undesirable consequences typically consists of addressing such categories as physical impacts to humans or the environment and economic impacts including mitigative and recovery costs associated with the physical impacts. Once the undesirable consequences are identified, the analyst may begin to identify the systems, processes, and hazards of interest that warrant further investigation. Commensurate with this approach, grading of hazards in the form of a conservative screening analysis is also important so as to allow the analyst to focus on the most significant hazards for further evaluation.

Common methods for initial identification of hazards include analyzing process/facility material properties and conditions,

reviewing analyses for other similar facilities, reviewing industry process experience, developing interaction matrices, and applying hazard evaluation techniques. The latter process often identifies additional hazards through methodical analysis and comparison of accident initiation, progression, and mitigation. For additional detail on application of these and other techniques, the student is referred to Chapter 3 of **Guidelines for Hazard Evaluation Techniques** by the American Institute of Chemical Engineers.

Rigor of analysis versus complexity of operation and potential consequences of accidents

The more complex the system or operation, the more potential for an undiscovered or missed interaction or sequence of events that could lead to a hazardous condition. As a corollary, if the accident consequences are unacceptably high for accidents identified during the analysis phase, a more thorough analysis may also be necessary to demonstrate acceptable risk. This would imply that a more thorough analysis would be required for complex, multiple system facilities or for facilities where accident consequences have the potential to be unacceptable high.

Conservative assumptions and documentation of assumptions

In order to have credibility, any analysis performed must make conservative assumptions where data found does not support modeling and analysis. Additionally, any and all assumptions must be documented in order to permit duplication and validation of results. If assumptions are made and are not documented, any validation of results through a peer review process becomes difficult if not impossible. Further, if conservative assumptions are not made, any results are compromised in terms of demonstrating acceptable risk. This is the mathematical equivalent of multiplying multiple factors, all but one of which are conservative. As a result, the answer is not conservative, in fact, the position on the spectrum is unknown. If this process is repeated with results of numerous individual series of calculations (cutsets) summed, the results of the sum are inconclusive since each individual calculated series is indeterminate. Stated another way, the sum if indeterminate cutsets results in an indeterminate summation.

Applicability of data

Where data are analyzed for input into an analysis, results are more credible if plant or facility specific data are available and analyzed. In the absence of plant or facility specific data, data from an identical or similar facility is next best, followed by data from site or facility installed equipment manufacturers, and finally, generic data from other facilities with similar missions and equipment but not necessarily similar processes. Often times generic data may only be available for use in analysis, but when used, careful consideration should be given to incorporating data from similar equipment of component designs. There are numerous public and private domain databases that have been specifically developed to support risk based quantitative analyses. Examples include IEEE-500 and the Savannah River historic equipment reliability database.

Consistency and control of any expert elicitation process (if used)

In order to maintain credibility in the data analysis phase of an assessment where either historic data are not available, or where the data are determined to be inappropriate for use, an expert panel is normally established and specific questions are asked in order to determine a best estimate point value and uncertainty (probability distribution) factor. This process must be documented and follow defined guidelines which generally involve elicitation of experienced analysts, operators and operations management/supervision, and engineering personnel to determine failure probabilities or other necessary data in order to support a thorough analysis. Credibility and accuracy of results are supported through consistency of process application and credibility of the expert panel and the ensuing data analysis and determination.

Validity and conservatism of scenario screening criteria

In the performance of detailed analyses, there are normally tens to hundreds of accident scenarios that may need to be analyzed. Upon identification of all credible initiators and accident scenarios, an initial screening is normally performed. This initial screening allows the analyst to focus on those accident scenarios which need to be modeled in detail for further study. This process must document the screening criteria and must always fail to a conservative approach when performing a scoping analysis of individual scenarios. Documenting the basis including any assumptions and the screening process allows the results to be duplicated thus establishing the validity of the initial accident screening process.

Reflection of lack of knowledge in uncertainty estimates
Uncertainty in data distributions is normally reflected in terms of an uncertainty estimate. Where data analysis indicates a wide distribution of (failure) data values, it is important to reflect this in the uncertainty (distribution) of data through the use of realistic or conservative uncertainty estimates. In probabilistic based analyses, uncertainty is normally given in terms of an error factor.

D. Review existing hazard analyses and assess the applicability methodology and recommendations/ conclusions resulting from the analysis.

As part of an exercise for this section, access an existing hazard analysis from the local DOE Field Office. Review the document and assess methodology, recommendations, and conclusions for applicability. Discuss results with your supervisor.

E. Discuss the applicability and pu rpose of nuclear and non-nuclear hazard analysis techniques required during the life cycle of a DOE facility.

As discussed in the various methods under Sub-section 1.B, the various hazard analysis techniques may typically lend themselves to more efficient application at various times during the facility life cycle. The analyst generally will determine which technique to use to analyze hazards/risks according to four primary variables:

1. cost
2. scope – including the scope of hazards as well as those initiators to be analyzed
3. complexity of the facility, structure, system or component
4. public or political interest.

These factors may often be interrelated and may require analyses and iteration in themselves to arrive at an acceptable method that will satisfy/address all issues. Table 5.3, on the following page, is a summary of prioritization attributes of the more common Hazard Evaluation techniques.

F. Discuss the benefits of applying hazard analysis techniques during the design phase of a facility, operation process or piece of equipment.

The process of applying hazard analysis techniques during the design phase of a facility, operation process, or component allows for either a qualitative or quantitative assessment of design criteria against desired performance attributes. The identification of sub-standard performance attributes appears in the form of excessive risk thus allowing for design modification prior to facility, operation process, or component construction. The hazard analysis process is generally iterative and may be repeated several times prior to design finalization. It seeks to modify design details to achieve desired safety objectives and thereby reduce risk and associated costs prior to construction and operation.

Table 5.3

Prioritization of Hazard Analysis Techniques

Technique	Provides Accident Scenario Information	Provides Frequency Information	Provides Consequence Information	Event Ranking Possible	Comments
PHA	May	No	Yes	Crude hazard category ranking	Usually ranked by hazard categories: Negligible; Marginal; Critical; or Catastrophic
HAZOP Analysis	Usually	May	Yes	Crude consequence ranking	Analysis performed by a team of individuals. Uses interaction and brainstorming techniques
FMEA	Usually	No	Yes	Crude qualitative consequence ranking; for quantitative see FMECA	FMEA generally qualitative; for quantitative priority ranking of failure severity see FMECA
FMECA	Yes	Yes	Yes	Priority ranking of failure severity	The criticality assessment in a FMECA provides a simple quantitative risk ranking
FTA	Usually	Yes, based on size and number of cut sets and type of failures involved	No	Frequency ranking based on analysis and comparison of multiple fault tree events	Quantitative FTA techniques are available to estimate top event frequencies
ETA	Yes	Yes, based on number of accident scenarios and number and type of failures involved	Yes, consequence categories are assigned for each scenario	Yes (Gross, unless combined with a more thorough top event analysis technique)	Quantitative ETA techniques are available to estimate top event and sequence frequencies. Example: ETA/FTA/HRA combined analysis
HRA	Yes	Yes, based on number and length of scenarios and type of human errors involved	No	Frequency Ranking	Quantitative HRA techniques are available to estimate human error probabilities. Often used in support of other analysis techniques

G. Discuss the importance of change control and its impact on the identification and timing of appropriate hazard analysis.

Change control is the continuous process of documenting as-designed/as-built facility equipment configuration and administrative and procedural changes. During the various stages of a facility life cycle, control over facility configuration documentation must be maintained since it forms the basis for and the validity of any hazard evaluation or risk assessment. Upon the completion of a hazard evaluation or risk assessment, issues are often identified which may require facility modernization or updates, redesign or re-engineering, deletion or addition of SSCs, or administrative or procedural modifications. As these issues are identified, existing design or as-built documentation must be modified to reflect a change in design or actual facility changes. Therefore, the process of hazard evaluation or risk assessment is used during all phases of a facility life cycle in an iterative sense. The hazard/risk evaluation process seeks to identify safety issues before they become a problem. Consequently, its use must be continuous, forming an integral part of the life cycle management process for a facility**.**

References and Suggested Reading

References and Suggested Reading

Henley, E. J. and Kumamoto, H., Probabilistic Risk Assessment, The Institute of Electrical and Electronics Engineers, New York, NY, 1992.

Guidelines for Hazard Evaluation Procedures, Center for Chemical Process Safety, American Institute for Chemical Engineers, New York, NY, 1992

Tukey, J. W., Exploratory Data Analysis, Addison-Wesley Publishing Co., Reading, MA, 1977.

Accident Analysis and Investigation

Section 6

OBJECTIVE

Demonstrate knowledge of accident causation theories as well as accident investigation, analysis, and reporting as practiced within the DOE.

1. Discuss accident causation models, emphasizing the importance of human reliability and effective management systems.

6 - 1

The job of DOE management and technical personnel is to identify the hazards that exist within the DOE facilities and eliminate or mitigate those hazards before accidents occur. In performing this work, it is important that these personnel have a fundamental understanding of the accident causation theories and its interpretation of the human factors and workplace variables which can result in accidents. This knowledge and awareness of these concepts will assist those DOE personnel in recognizing and communicating the safety problems to the facility management and technicians.

Single Factor Theory

This theory is very limited in that it assumes that every accident has only a single and simple cause. An application of this theory can be demonstrated by reviewing what causes a forklift operator puncturing a radioactive storage drum. According to this theory, the cause of the accident is the forklift. Yet, by identifying this cause would not mitigate or stop the problem. This theory fails to look at other contributing factors such as worker training, storage method, or corrective actions. This myopic focus makes this theory useless for accident and loss prevention.

Domino Theories

There are three different domino theories of accident causation: Heinrich's, Bird and Loftus', and Marcum's Domino Theories. Each domino theory presents a different explanation for the cause of accidents, however, each theory is predicated on the fact that there are three phases to any accident. The three phases are the pre-contact phase, the contact phase and the post contact phase.

The pre-contact phase are the events or conditions that lead up to the accident.

The contact phase is the phase when the accident actually occurs.

The post-contact phase refers to the results of the accident.

Domino theories represent accidents as causal factors or hazard events. Each causal factor affects the others if allowed to build up over time (pre-contact phase). Without intervention, the hazards will interact to cause the accident and move into the contact phase. Thus the derivation of the theory's name as Domino.

Heinrich's Domino Theory

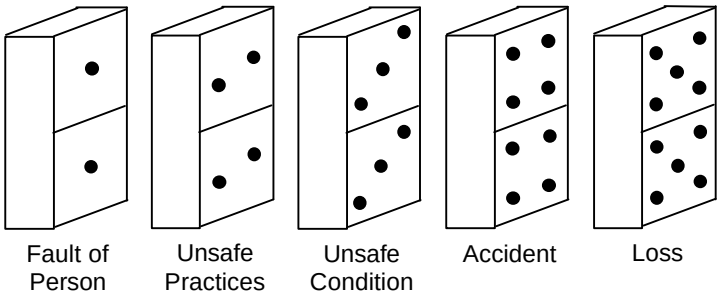
Heinrich's domino theory essentially states that there are five series factors that could influence an accident. The factors occur sequentially and consist of the following:

1. A negative trait or factor is present in a person as a result of social influence of environment
2. The negative trait or factor may lead to an unsafe practice or condition
3. The unsafe practice results in an unsafe condition, or it results in mechanical or physical hazards that are the direct cause of an accident
4. Accidents that result from the above process are typically the result of falls or impacts with other moving objects
5. Injuries from above are usually of the form of lacerations and fractures.

As a result of this process, intervention or elimination of any of the first four factors will stop the injury or loss.

Heinrich's Domino Theory

Figure 6.1



Bird and Loftus' Domino Theory

Similar to the Heinrich's Theory, this theory states that there are five series factors that could influence an accident. However, this theory states that the ultimate responsibility for the welfare of the employees lie with the management of an organization. It is the manager of the organization who can instill the controls necessary to prevent the initiation of the domino effect.

Bird and Loftus' Domino Theory

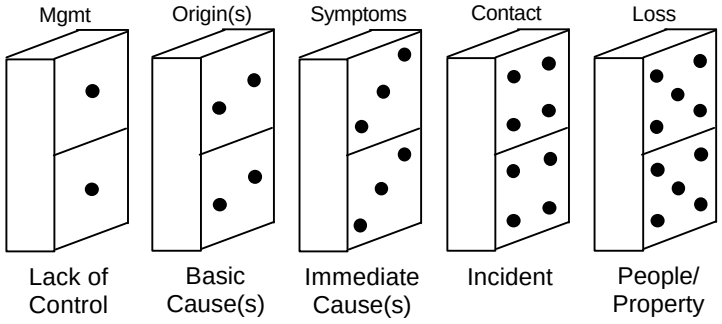


Figure 6.2

1. Lack of Control - Management
   Control in this instance refers to the four functions of a manager: planning, organizing, leading and controlling. Examples of this domino are purchasing substandard equipment or tools, not providing adequate training, or failing to install adequate engineering controls.
2. Basic Cause(s) - Origin(s)
   The basic causes are frequently classified into a personal factors group and a job factors group. Personal factors may be lack of knowledge or skill, improper motivation, and physical or mental problems; job factors include inadequate work standards, inadequate design or maintenance, normal tool or equipment wear and tear, and abnormal tool usage.
3. Immediate Cause(s) - Symptoms.
   The primary symptoms of all incidents are unsafe acts and unsafe conditions.
4. Incident - Contact
   An undesired event occurs. The accidents are often represented by the eleven accident types in Table 6.1.

Eleven Accident Types

Table 6.1

stuck-by	caught-in	fall-to-below
struck-against	caught-on	overexertion

contact-by	caught-between	exposure
contact-with	foot-level-fall	

source: ANSI Z 16.2

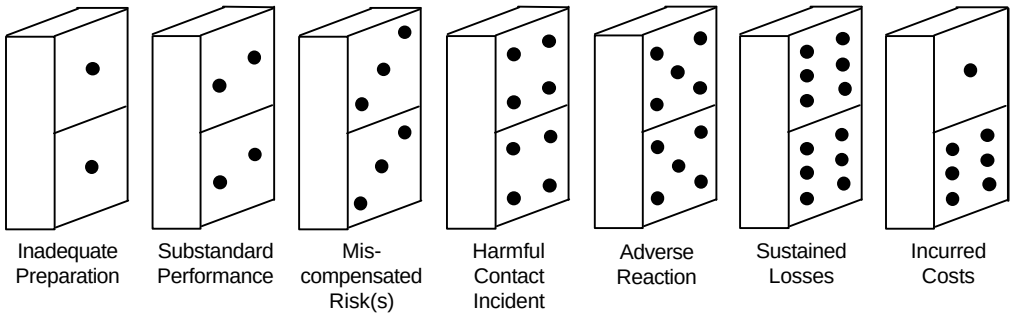
5. People – Property – Loss
   Result of the accident. The effects are property or environment damage or injury to personnel.

Marcum's Domino Theory

According to C. E. Marcum's 1978 Seven Domino Sequence of Misactsidents, a misactsident is an identifiable sequence of misacts associated with *inadequate task preparation* which could lead to *substandard performance* and *miscompensated risks*. Marcum also includes the cost aspect of a loss. Like the previous theory, Marcum states that management is ultimately responsible to ensure that the workplace is designed with adequate controls to protect employee.

Figure 6.3

Marcum's Domino Theory



Through this domino theory, Marcum shows that accidents can be prevented by the management by properly training the employees as well as designing adequate controls into the work process.

Multiple Causation Accident Theories

Multiple Factors Theory

The multiple factors theories use four M factors, as shown in Table 6.2, to represent causes of accidents. Multiple factors theories attempt to identify the hazardous condition (pre-contact) that exist in an operation by revealing the causes that will lead to an accident.

Table 6.2

Grose's Accident Factors

Factor	Description	Characteristics

Machine	tools, equipment, or vehicles that may contribute to an accident	design, shape, size, specific type of energy used to operate equipment
Media	environmental conditions surrounding an accident: weather, walking surface	gender, age, height, weight, condition, memory, recall, knowledge level
Man	people and human factors that could contribute to an accident	snow or water on a roadway, temperature of a building, outdoor temperature
Management	method used to select equipment, train personnel, or ensure a relatively hazard-free environment	safety rules, organization structure, policy and procedures

Systems Theory of Causation

This theory states that the probability of an accident lies with how the worker, machine, and environment interact with each other. For example the knowledge, skills, and ability, whether acquired through training or gained from years of experience, influences the way a person deciphers the information regarding the environment as well as how he will use the machinery. This, in effect, will affect his decision making and therefore will have a bearing on the person performing a job and therefore influence the probability of a mishap.

Psychological/Behavioral Accident Causation Theories

Goals Freedom Alertness Theory

According to this theory, accidents are the result of low-quality worker behavior. Correction to this behavior is in the form of raising worker awareness through a positive organizational culture and psychological climate. For example, ensuring that workers are disciplined to maintain good housekeeping will reduce mishaps.

Motivation Reward Satisfaction Model

This theory builds upon the previous theory. According to this theory, rewards are the factor that have the greatest effect upon performance. If rewards are fairly disseminated as perceived by the employees, there is an increased likelihood of motivation which will produce positive safety results. For example, one of the DOE sites decided to implement a program where a pool of safety fund is allotted at the beginning of the year. For every accident, a certain amount of money is reduced from the original allocation. Then at the end of the year, the remaining funds,

if any are divided up among the employees. Since starting this program, the number of mishaps have decreased significantly.

Human Factors Theory

This theory is based on the fact that human errors cause accidents. The three human factors which can lead to human errors are overload, inappropriate activities, and inappropriate response.

Overload can occur when a person must perform excessive number of tasks. Despite whether this person is qualified or not, it is the overburden situation which creates the scenario for a mishap.

An inappropriate activity can occur when a person is not adequately trained to perform his duties. This is one of the reasons for ensuring that any trainee performing a “real” task during an on-the-job training is supervised at all times.

An inappropriate response occurs when a qualified person purposely violates a procedure for productivity or he fails to correct the problem when it is detected.

Energy-Related Accident Causation Theories

Energy Release Theory

According to this theory, an accident is caused by a lack of engineering control. This lack of control results in energy that is out of control which puts causes stress limits to be violated, whether on a person, machinery, or environment. Therefore, accidents can be prevented by instilling a proper engineering control to divert the energy, which is the source of the hazards.

6 - 2

2. Discuss the purpose of accident investigation within the DOE. Discuss the DOE accident investigation methodology.

Purpose

According to DOE Order 225.1, the purpose of accident investigation is to improve the environment, safety and health for DOE employees, contractors, and the public. A second purpose is to prevent recurrence of accidents.

Accident Investigation

The DOE accident investigation contains four main steps:

1. Categorization
2. Conduct the Investigation
3. Report Investigation Results
4. Investigation Close-Out.

Step 1 Categorization

DOE accidents are categorized as warranting either a Type A or a Type B investigation. The algorithm for determining the type of investigation is found under objective 2.A. The categorization algorithm is also found as Attachment 2 to DOE Order 225.1.

Step 2 Conduct the Investigation

The first step in a DOE accident investigation is the appointment of the Accident Investigation Board. The investigation time frame and board participants are outlined in DOE Order 225.1. The Board's composition is mandated based upon the type of investigation; this information is found in the Order. The second step is the actual accident investigation which is detailed under objective 2.B. The main objective of the investigation is to analyze the facts and identify causal factors and judgments of need for corrective actions.

Step 3 Report Investigation Results

After the Board has prepared the report, it is submitted to the Appointing Official who then accepts the report and its findings. The investigative phase is complete at this point. The investigation report's purpose and content is handled in detail under objective 2.E.

Step 4 Investigation Close-Out

The Appointing Official ensures that the DOE and contractor line management organizations affected by the investigation have had an opportunity to conduct a factual accuracy review of the draft report and present comments to the Board. The Board Chairperson and the senior manager of the site conduct a formal briefing on the outcome of the investigation. The final report is given to senior managers with a request for their organizations to prepare corrective action plans. The lessons-learned from the accident investigation are disseminated DOE-wide. Last, the action plans are completed, and corrective actions are implemented to satisfy the judgments of need identified in the final investigation report.

A. Discuss and demonstrate the ability to apply the criteria for determining the need for a particular type of accident investigation.

DOE Order 225.1 provides an accident investigation categorization algorithm as Attachment 2. This algorithm provides the criteria for categorizing an accident investigation as either a Type A or a Type B investigation. A table representation of the algorithm is found as Table 6.3. It breaks the criteria into four difference categories of effects: Human, Environmental, Property, and Other.

Table 6.3

Accident Investigation Categorization Algorithm

TYPE A INVESTIGATION	TYPE B INVESTIGATION
Human Effects	
Any fatal, or likely to be fatal, injury, chemical or biological exposure to an employee or a member of the public	Any one or series of injuries, chemical exposures, or biological exposures that results in hospitalization of one or more employees or members of the public for more than 5 continuous days
Any one accident that requires the hospitalization for treatment of 3 or more individuals	Any one or series of injuries, chemical exposures, or biological exposures that results in permanent partial disability of one or more employees or members of the public
Any one accident that has a high probability of resulting in the permanent total disability due to injuries, chemical exposures, or biological exposures of DOE, contractor, or subcontractor employees or members of the public	Any one accident or series of accidents within a 1-year time period, resulting in 5 or more lost-workday cases, or any series of similar or related accidents involving 5 or more persons, one or more of which is a lost-workday case.

A single individual radiation exposure resulting in: a. A total effective dose equivalent > 25 rem b. A dose equivalent to the lens of the eye > 75 rem c. A shallow dose equivalent to an extremity or skin > 250 rem d. The sum of the deep dose equivalent for external exposure and the committed dose equivalent to any organ or tissue other than the lens of the eye > 250 rem e. A dose equivalent to the embryo or fetus of a declared pregnant worker > 2.5 rem	A single radiation exposure to an individual that results in: a. A total effective dose equivalent > 10 but < 25 rem b. A dose equivalent to the lens of the eye > 30 but < 75 rem c. A shallow dose equivalent to an extremity or skin > 100 but < 250 rem d. The sum of the deep dose equivalent for external exposure and the committed dose equivalent to any organ or tissue other than the lens of the eye > 100 but < 250 rem e. A dose equivalent to the embryo or fetus of a declared pregnant worker > 1 but < 2.5 rem
Environmental Effects	
Release of a hazardous substance, material, waste, or radionuclide from a DOE facility (onsite or offsite), in an amount greater than 5-times the reportable quantities specified in 40 CFR Part 302, that results in serious environmental damage	Release of a hazardous substance, material, waste, or radionuclide from a DOE facility (onsite or offsite), in an amount ≥ 2-times but < 5-times the reportable quantities specified in 40 CFR Part 302, that results in serious environmental damage
Property Effects	
Estimated loss of, or damage to, DOE or other property, including aircraft damage, ≥ $2.5 million or requiring estimated costs ≥ $2.5 million for cleaning, decontaminating, renovating, replacing, or rehabilitating structures, equipment, or property	Estimated loss of, or damage to, DOE or other property ≥ $1 million but < $2.5 million, including aircraft damage, and costs of cleaning, decontaminating, renovating, replacing, or rehabilitating structures, equipment, or property
Any apparent loss, explosion, or theft involving radioactive or hazardous material under the control of DOE, contractors, or subcontractors in such quantities and under such circumstances to constitute a hazard to human health and safety or private property	The operation of a nuclear facility beyond its authorized limits
Any unplanned nuclear criticality	
Other Effects	

Any accident or series of accidents for which a Type A investigation is deemed appropriate by the Secretary or the Assistant Secretary for Environment, Safety and Health.	Any accident or series of accidents for which a Type B investigation is deemed appropriate by the Secretary; Assistant Secretary for Environment, Safety and Health; Associate Deputy Secretary for Field Management; Cognizant Secretarial Officer; or Head of the Field Element. This includes Departmental cross-cutting issues and issues warranting the attention of local news or interest groups.

B. Discuss and apply the necessary techniques for gathering the facts applicable to a given investigation .

DOE Order 225.1 lists the information that should be gathered by the accident investigation board during an investigation.

> The Board shall be responsible for conducting a thorough investigation of all individuals, organizations, and facilities having a stake in the accident.
>
> The Board shall determine the facts of the accident by examining the accident scene, examining DOE and contractor documentation, interviewing witnesses, and performing engineering analyses. The Board shall also examine policies, standards, and requirements that are applicable to the accident being investigated as well as management and safety systems at Headquarters and Field Offices that could have contributed to or prevented the accident.

The purpose of an accident investigation is to determine the causes of the accident. Once the causes are determined, this information will then be fedback to the management, who will then take corrective actions by training the workers or instilling new controls to prevent similar accidents.

All accident investigation should be for the sake of fact finding and <u>not</u> fault finding.

Investigation should be conducted using the who, what, where, when, how, and why questions. For example:

1. Who are the victims?

2. What events lead up to the accident?
3. Where was equipment and/or machinery?
4. When did the incident occur?
5. How did the victims and witnesses react in given situations?
6. Why did the incident take place, in your opinion?

Interviews and document reviews will be the main source of information. However, observations of the place of the accident and the surrounding areas will be invaluable in determining the setting and the environment leading to the accident. All these factors are important to finding the cause as discussed through the use of the various accident theories.

C. Discuss the purpose and content of an accident investigation report.

DOE Order 225.1 outlines the purpose and content of the report. The purpose of the report is to contain the investigation board's judgment on the need for corrective actions based upon objective analysis of the facts, root and contributing causes, and DOE or contractor management systems that could have prevented the accident. The report will not contain statements that determine individual fault or propose punitive measures.

The facts section of the draft investigation report should be offered to the affected DOE and contractor line management for their review of the report's factual accuracy. Prior to completing the investigation, the accident investigation board will review the report to ensure its technical accuracy, completeness and internal consistency. They will also include an analysis of management control and safety systems that may have contributed to the accident.

If a board member wishes to offer an opinion different from that of the investigation board, a minority report section can be added to the report.

D. Discuss the importance of providing feedback based on accident investigations, and describe the management systems necessary to ensure the communication of this feedback to the Department.

Since the DOE operates numerous sites across the country, it is paramount that information learned in the course of an accident investigation be shared throughout the DOE and its contractors. Through the communication and dissemination of accident information which includes lessons learned and corrective actions, all sites benefit. In addition, other sites may analyze their facilities for similar problems and implement needed changes in order to avoid a similar accident or occurrence. When practiced, this process saves lives and money by avoiding repeated accidents.

One of the main tools used to accomplish the communication of accident and occurrence information is the Occurrence Reporting and Processing System (ORPS). This system serves as a historical database for all accident and occurrence report information within the DOE and its contractors. Once the information is stored in ORPS, the DOE Office of Environment, Safety and Health in conjunction with the Office of Nuclear Facility Safety publishes the Operating Experience Weekly Summary. The process is intended to disseminate lessons-learned information as described in DOE-STD-7501-95. In addition to ORPS, the Office of Operating Experience Analysis and Feedback compiles information from daily operations reports, notification reports, and conversations with DOE field office and facility staffs for inclusion in the Weekly Summary. This effort is intended to augment ORPS but should not substitute for a thorough review of interim and final occurrence reports.

References and Suggested Reading

References and Suggested Reading

Bird, F. E., and Loftus, R. G., Loss Control Management, Institute Press, Loganville, GA, 1976.

Department of Energy, DOE Order 225.1, DOE, 1996.

Kohn, J. P., Friend, M. A., and Winterberger, C .A., Fundamentals of Occupational Safety and Health, Government Institutes, Inc. Rockville, MD, 1996.

Nuclear Safety Analysis

Section 7

OBJECTIVE

Demonstrate knowledge of nuclear risk management and hazard assessment to ensure that program priorities are established, formal process requirements are met, and resources are applied to ensure safety of operations, as described in DOE Order 5480.22, Technical Safety Reports, and DOE Order 5480.23, Safety Analysis Reports.

7 - 1

1. Demonstrate knowledge of nuclear risk management and hazard assessment to ensure that program priorities are established, formal process requirements are met, and resources are applied to ensure safety of operations, as described in DOE Order 5480.22, Technical Safety Reports, and DOE Order 5480.23, Safety Analysis Reports.

A. Define and compare the terms *risk* and *hazard*.

A **hazard** is a source of danger with the potential to cause illness, injury, or death to personnel, to damage an operation, or to damage the environment. The sources of danger can be material, energy sources or operations.

Risk is the quantitative or qualitative expression of possible loss that considers both the probability that an event will occur and the consequences of that event.

The relationship between risk and hazard can be expressed as Hazards ⌫ Protection ⌫ Risk

Hazards Sources of Risk	Protection Prevention of Loss or Damage
• combustible materials	• fire extinguishers
• high pressure piping	• pipe restraints
• chemical solutions	• protective clothing
• radionuclide inventories	• decontamination facilities
• potential energy such as dams	• emergency planning
• biological hazards.	• vaccinations.

Risk Assessment and Hazard Evaluation

The two techniques for evaluating risk and hazards are risk assessment and hazard evaluation. Actually the distinction between the two is arbitrary since both address the three basic questions of "What could go wrong?", "How likely is it to go wrong?" and "What are the consequences?".

Hazard evaluation is often associated with methods that provide qualitative answers while risk assessment is applied to techniques that render quantitative answers. The purpose behind both hazards analysis and risk assessment is to learn from experience in order to reduce the probability of future accidents. These two techniques help us to look, think and make decisions regarding the safety disposition of a facility. Last, they are employed in response to legislative and regulatory requirements.

B. Discuss the factors that can affect risk.

The main factors that affect risk for DOE nuclear and nonreactor nuclear facilities are the probability of release and the severity of the consequences. Risk can be depicted as a matrix of probability vs. severity as shown in Figure 7.1 on the following page.

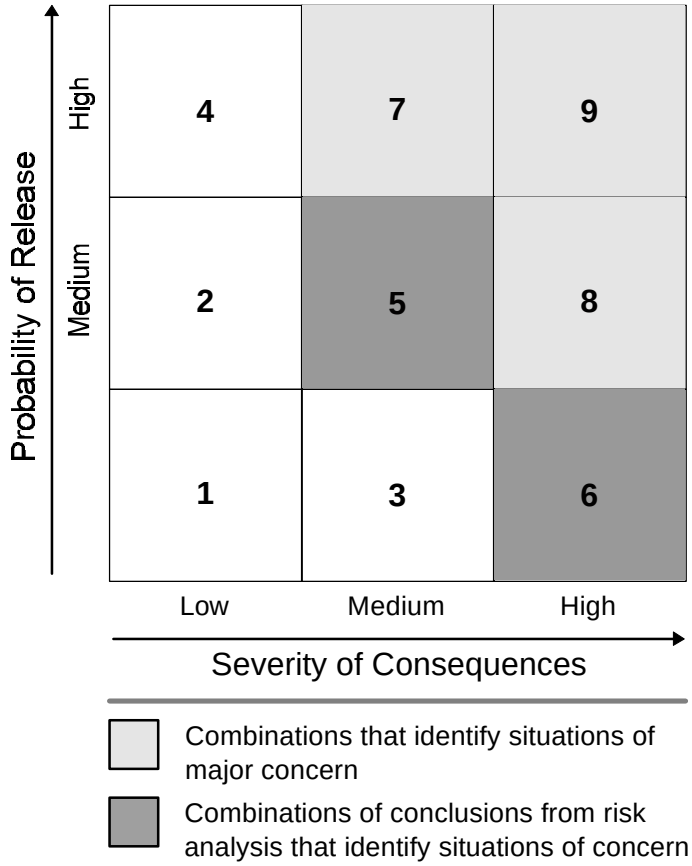
Since risk is the product of frequency and consequence, the factors that affect risk are broken down into those which affect frequency of a hazard or accident and those which affect consequence.

Factors that Affect Frequency

- Effective ORPS Management and Lessons Learned Program
  This process seeks to identify and disseminate those indicators, manufacturing details or other common flaws including maintenance and operations procedures which have led to near misses or actual accidents. The goal is the widest possible dissemination of information.
  Effective Risk Management Program: Such a program is intended to actively and continuously identify, analyze, prevent, and mitigate accident scenarios that result in unacceptable risk.
  Effective Conduct of Operations Program: Training and procedures which emphasize the formality of communications and operations can reduce risk by minimizing initiation frequencies resulting from human error.

Risk: Probability and Consequence Ranking Matrix for Hazard Evaluation

Figure 7.1



Factors that Affect Consequence

- Siting
  During the design phase, siting plays an important role in consequences according to surrounding site population density. Additionally, siting demographics including highways and road traffic densities may significantly change during the facility's lifetime. Reanalyzes with respect to these changes in static and dynamic populations may also be significant factors for consequence.
- Emergency Management Program
  An emergency response program for both the site and the surrounding area are essential. An effective program reduces consequences by minimizing those effects of public exposure through evacuation routing, PPE, and exposure monitoring.
- Formal Training
  Training on consequences of accidents should identify those activities that minimize consequences. For example, in order to reduce the consequence of radiation exposure, training should be conducted on shielding concepts.
- Risk Management Program
  A proper risk management program seeks to identify the hazard sources and quantity as well as the significance and the consequences. An effective program will manage risk and therefore the consequences.
- Hazardous Inventory Management
  An effective program seeks to minimize the amount of hazardous inventory to that necessary to achieve the facility's goals.
- Weather and other environmental conditions
  These factors affect plume and dispersion of hazardous materials which alternatively lead to exposures and environmental contamination.

C. Explain and compare the terms *design basis* and *authorization basis*.

Design Basis

The *design basis* is the set of requirements that constrain the design of systems, structures, and components (SSCs) within a facility. These design requirements include safety considerations, plant availability, efficiency, reliability and maintainability. Not all design

basis aspects are important to safety. *Design Basis Accidents* are the accidents which are postulated for the purpose of establishing functional requirements for safety-significant SSCs and equipment.

Authorization Basis

The *authorization basis* are those aspects of the facility design basis and operational requirements that DOE applies to authorize facility operation. These aspects are important to safety. The authorization basis is described in the facility Safety Analysis Report (SAR), Hazard Classification Documents, Technical Safety Requirements (TSR), Safety Evaluation Reports, and facility-specific commitments made in order to comply with DOE Orders and policies.

Safety Basis

When discussing safety of operations in terms of SARs and TSRs it is necessary to define the term *safety basis*. This basis is the combination of information which relates to the control of hazards at a nuclear facility. This information includes design, engineering analyses, and administrative controls. DOE uses this information to conclude that the facility safely conducts its activities. The safety basis is the basis for accepting the risk of operation

It is the *safety analysis* that develops and evaluates the adequacy of the safety basis for facility. It is a documented process that:

- provides systematic identification of hazards within a given DOE operation
- describes and analyzes the adequacy of measures taken to eliminate, control or mitigate identified hazards
- analyzes and evaluates potential accidents and their associated risks.

While the *safety basis* closely resembles the *design basis*, it is a broader concept. The term safety basis includes the design basis in addition to safety commitments such as conceptual design, safety objectives, formal quantitative definition of safety performance criteria, commitments to engineering codes and standards, equipment qualification requirements, configuration controls, and the bases for and contents of TSRs. The safety basis also embraces the managerial, institutional, and human factors dimensions of safety assurance since the safety of DOE's nuclear facilities requires a balance of institutional and engineering approaches.

Safety Envelope

The *safety envelope* is a technically justified set of bounds on a facility's operations and design. The technical justification is derived from the accident analysis performed during the safety analysis while the safety envelope is substantiated and supported by the safety basis. The safety envelope consists of

- the operating envelope which is a set of limits or bounds within which all operations are conducted
- the design envelope which is a set of design commitments developed to support the facility as it exists and is actually operated.

DOE manages facility risk by ensuring that the activities performed are within the safety envelope as defined by the safety basis.

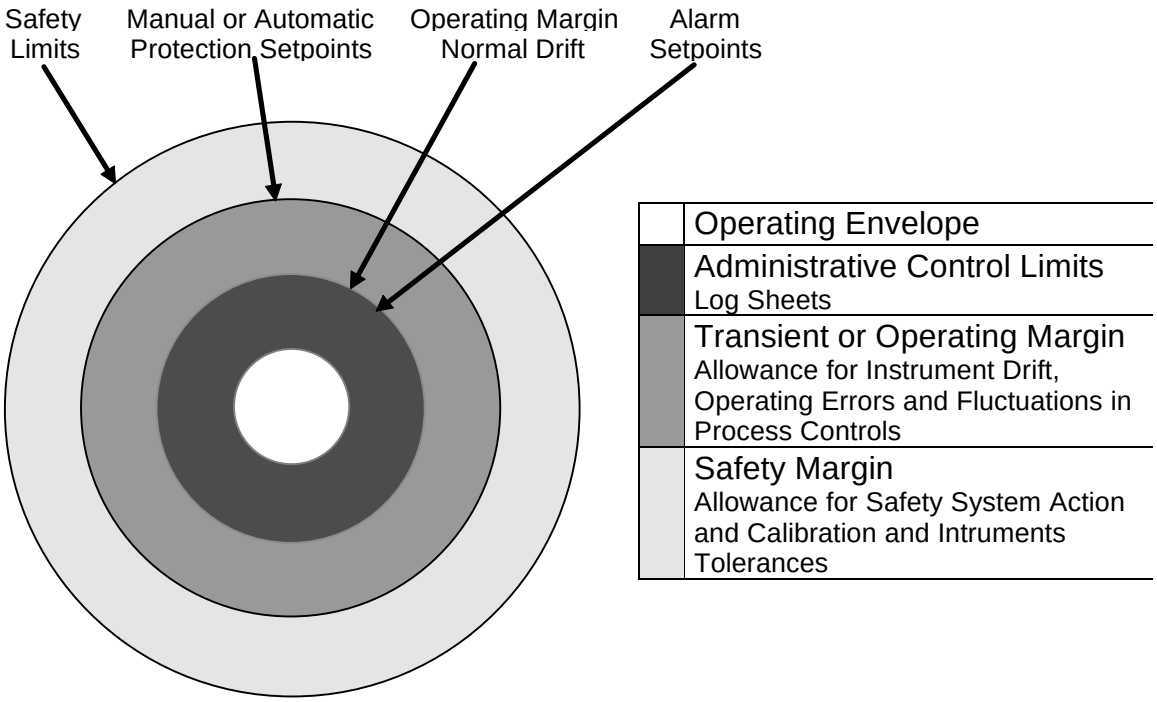
Margin of Safety

The *margin of safety* is an agreement between DOE or its appointed facility regulator and the facility operator. The regulatory process establishes safety-related limits on various variables and conditions. The operator agrees to operate within these limits and to install and maintain systems to ensure such operations.

Figure 7-2 depicts the envelopes and margins discussed in the previous paragraphs.

Envelopes and Margins

Figure 7.2



D. Identify the organization/individual that can change the authorization basis.

DOE Order 5480.23, Nuclear Safety Analysis Reports, does not explicitly identify the organization or individual who can change the authorization basis.

Paragraph 7.a covers the Secretary's Responsibilities and Authority.

> Many provisions in this Order permit and/or necessitate the exercise of discretion and/or judgment in carrying out the requirements of the Order. In those instances, the determination of whether, in the exercise of such discretion and/or judgment, the requirements of this Order were compiled with rests initially with the relevant Department authority, and, ultimately with the Secretary.
>
> The Secretary retains the sole and final authority to determine what acts are necessary to comply with this Order. Further, the Secretary retains the authority to suspend any and all requirements under this Order whenever the Secretary deems it necessary. This authority may be delegated by the Secretary as appropriate.

Paragraph 7.b.2 does state that Secretarial Officers or their designees in the line management shall

> …review and approve Safety Analysis Reports and revisions thereto for all nuclear facility and operations. The Secretarial Office shall issue a Safety Evaluation Report that documents the bases upon which the approvals have been made. The Safety Analysis Report, Safety Evaluation Report, and the Technical Safety Requirements Document, and any facility-specific commitments made in order to comply with DOE nuclear safety Orders or policies constitute the nuclear safety facility authorization from DOE for the contractor to operate the facility.

E. Discuss the purpose and the roles and responsibilities of the technical manager for the following:

- **DOE Order 5480.22, Technical Safety Requirements**
- **DOE Order 5480.23, Nuclear Safety Analysis Reports**
- **DOE Order 425.1, Startup and Restart of Nuclear Facilities**
- **DOE Order 232.1, Occurrence Reporting and Processing of Operations Information**
- **DOE Standard 3006-93, Planning and Conduct of Operational Reviews**

DOE Order 5480.22 clearly states the requirement to have Technical Safety Requirements (TSRs) prepared for DOE nuclear facilities and to delineate the criteria, content, scope, format and approval process, and reporting requirements of these documents and their revisions. The roles and responsibilities of the technical manager are to:

- prepare TSRs for the facility
- submit TSRs to the Program Secretarial Office (PSO) for approval
- operate the facility in accordance with TSRs as approved and/or modified by the PSO
- keep Technical Safety Requirements current so they reflect the facility as it exists and as it is analyzed in its Safety Analysis Reports.

DOE Order 5480.23 establishes the requirement for contractors responsible for the design, construction, operation, decontamination, or decommissioning of nuclear facilities to develop safety analyses that establish and evaluate the adequacy of the safety basis of the facilities. The order also requires a Nuclear Safety Analysis Report

(SAR) to document the results of the safety analysis. The roles and responsibility of the technical manager are to:

- perform a safety analysis that develops and evaluates the adequacy of the safety basis for a facility
- include in the safety analysis management, design, construction, operation, and engineering characteristics necessary to protect the public, workers, and the environment from the safety and health hazards posed by the facility
- adhere to the assumptions and commitments set forth in the safety analysis
- identify assumptions in accident analyses about initial conditions of facility operation that might prevail prior to an accident
- identify assumptions made in institutional safety programs such as quality assurance or surveillance
- prepare and submit to DOE a Safety Analysis Report which documents the safety analyses
- maintain up-to-date analyses of the safety of the facility and document the analyses in a form that is auditable by DOE

DOE Order 425.1 establishes the requirements for startup of new nuclear facilities and for the restart of existing nuclear facilities that have been shutdown. The order specifies a readiness review process which demonstrates that it is safe to startup or restart the facility. A second purpose of the order is to define the process for documented, independent operational readiness reviews and readiness assessments of the facility seeking to startup or restart. The functions of the technical manager are to:

- determine if an Operational Readiness Review (ORR) is required for startup of a new facility or restart of a nuclear facility
- determine if a Readiness Assessment (RA) is required if an ORR is not required
- prepare startup/restart notification reports, plans-of-action, Operational Readiness Review Implementation Plans and the Final Report
- establish adequate and correct procedures and safety limits for operating the process systems and utility systems
- implement training and qualification programs for operations and operations support personnel

- describe the safety envelope of the facility through facility safety documentation which
- characterize the hazards and risks associated with the facility
- identify mitigating measures that protect workers and the public from those hazards and risks
- define safety systems and other systems essential to worker and public safety
- maintain control over the design and modification of facilities and safety-related utility systems
- implement a program that confirms and periodically reconfirms the condition and operability of safety systems
- identify, evaluate, and resolve deficiencies and recommendations made by oversight groups, official review teams, and audit organizations
- systematically review the facility's conformance to applicable DOE Orders, identify any non-conformance, and schedule obtaining compliance
- establish management programs to ensure operations support services are adequate for operations
- establish and implement a routine and emergency operations drill program
- create an adequate startup or restart test program that provides for graded operations testing to confirm the operability of equipment, the viability of procedures, and the training of operators
- define and implement functions, assignments, responsibilities, and reporting relationships that will support line management's responsibility for the control of safety
- implement DOE Order 5480.19, Conduct of Operations Requirements for DOE Facilities
- ensure adequate staffing of qualified personnel to support safe operations
- promote a site-wide cultural awareness of public and worker safety, health, and environmental protection
- ensure that facility modifications are consistent with facility systems and procedures
- ensure that the breadth, depth and results from Operational Readiness Reviews are adequate to verify the readiness of hardware, personnel, and management programs for operations

- review facility modifications for potential impacts on procedures, training and qualification; revise procedures and training to reflect the modifications

DOE Order 232.1 establishes the occurrence reporting requirements for DOE elements and contractors responsible for the operation of DOE-owned and operated facilities. The requirements of the order include categorization of occurrences that have potential safety, environmental, health, or operational significance, DOE notification of these occurrences, and the development and submissions of follow-up reports. The roles and responsibility of the technical manager are to:

- categorize the event
- notify the DOE Facility Representative and the HQ Emergency Operations Center of Unusual Occurrences
- prepare and submit a Notification Report
- prepare and submit an Update Report when significant and new information is available or upon the request of DOE
- document any changes in categorization in an Update Report
- prepare and submit a Final Report when the root cause of the occurrence has been analyzed, corrective actions determined and schedules, and lessons learned identified
- resubmit a revised Final Report if the original Final Report is rejected by either the Facility Representative or the Program Manager.

DOE Standard 3006-95 provides guidance on the approved approaches and methods for implementing the requirements of DOE Order 425.1, Startup and Restart of Nuclear Facilities. The standard also describes a consistent approach to conducting Operational Readiness Reviews (ORRs) and Readiness Assessments (RAs) for new starts and restarts of DOE nuclear facilities. Last, the standard provides guidance on implementing ORRs and procedures to manage RAs. The technical manager's roles and responsibilities under the standard are the same as those under DOE Order 425.1. The following methods and approaches are detailed in DOE-STD-3006-95:

- determine the type of readiness review which is appropriate to the specific facility startup

- develop the breadth and depth (scope) of the ORR or RA in a manner that is consistent with the history, hazards, and complexity of the facility being started up
- develop procedures and conduct an ORR or RA for startup of a specific activity
- verify that the facility is physically ready to startup
- verify that the managers and operators are prepared to manage and operate the facility in the phase in which it is about to startup
- verify that the necessary infrastructure (procedures, staffing, compliance with DOE orders, rules and other requirements) is in place
- prepare requests for exemptions from the requirements of DOE Order 425.1

F. Discuss the interface/relationship between the above Orders.

Relationship between 5480.23 and 5480.22

The safety analysis conducted under the guidance of DOE Order 5480.23 should furnish a logical basis for the comprehensive definition of the acceptable operating envelope for a nuclear facility as well as the information necessary to validate, confirm, derive, or modify the basis of the Technical Safety Requirements whose derivation, scope and contents are established in DOE Order 5480.22. The relationship between the SAR and the TSR is examined in more detail in objective 1.I.

Relationship between DOE Orders 425.1, 5480.23 , 5480.22 and DOE-3006-95

DOE Order 425.1, Startup and Restart of Nuclear Facilities, specifies that an Operational Readiness Review will be conducted for the restart of a nuclear facility shutdown due to operations outside the safety basis. The safety basis is documented in DOE Order 5480.23 and supported by TSRs generated as specified in DOE Order 5480.22. (Paragraph 4.1.1.e) Part of the minimum core requirements for an ORR includes the facility safety documentation that describes the safety envelope of the facility. This documentation should characterize the hazards and risks associated with the facility, and it should identify mitigating measures that protect workers and the public from these hazards and risks. (Paragraph 4.d.4) DOE-STD-3006-95 provides

guidance on the approved approaches and methods for implementing the requirements of DOE Order 425.1.

Relationship between DOE Orders 232.1 and 5480.22
DOE Order 232.2, Occurrence Reports and Processing Operations Information, discusses Unusual Occurrences in Paragraph 2. An unusual occurrence is a non-emergency occurrence that exceeds the off-normal occurrence threshold criteria and is related to safety, environment, health, security or operations. The order provides the types of occurrences that are categorized as Unusual, and paragraph 2.k contains the interface to the TSR.

> Reduction of the safety margin below that prescribed in the authorization basis of a facility or process (including violations and noncompliances of Technical Safety Requirements, Operational Safety Requirements, Technical Specification, or other authorization basis documents.)

G. Identify the purpose and discuss the basic content elements of a Safety Analysis Report (SAR).

The Safety Analysis Report documents the adequacy of the safety analysis for a nuclear facility, and it ensures that the facility can be constructed, operated, maintained, shut-down, and decommissioned in compliance with applicable laws and regulations.

SAR Scope

- defines the safety basis, documents the logic of its derivation, demonstrates adherence to the safety basis, and justifies its accuracy
- includes thorough documentation of the assumptions employed in the safety analysis
- includes the results of the safety analysis that identifies the dominant contributors to facility risk so these vulnerabilities can be better managed.

SAR Objectives

1. provide the bases for approval of new facilities and operations, major modification to existing facilities, and eventual decommissioning

2. define and control the safety basis and commitments
3. support safety oversight of facilities and operations
4. provide the analytical rationale for operations as delineated in the TSRs.

SAR Contents

The contents of the SAR as well as the level of effort necessary to create and maintain a SAR, the sophistication of the analyses that go into its preparation, and the thoroughness of the documentation in the submitted SAR should be proportioned by three factors:

1. the magnitude of the hazards being addressed
2. the complexity of the facility and systems being relied on to maintain an acceptable level of risk
3. the stage or stages of the facility life cycle for which DOE approval is sought.

SAR and Day-to-Day Operations

The guidance attachment to DOE Order 5480.23 contains insight into the role of the safety analysis and the SAR in recording the DOE-contractor consensus on how safety is safeguarded in ongoing nuclear operations. The purpose of the analysis and the SAR is not just to support the initial safety review and approval for new facilities. It also defines the basis for continuing operations. SARs must be kept up-to-date as facilities are changed or modified. It is through the process of updating, upgrading and amending the SAR that the contractor updates its safety commitments to DOE and ensures the safety of both the facility and its operations.

SARs become practical for day-to-day operations. Basically, the SAR must become a living document that conveys management's commitments to safe operations.

SAR and the Safety Analysis Process

The DOE Order also upgrades the requirement of the analysis to employ recent advances in state-of-the-art analysis. Example analyses cited in the order include:

- risk assessment
- severe accident analysis

- system reliability analysis
- common cause failure analysis
- techniques in human factors safety analysis
- human reliability analysis.

Figure 7-3 outlines the DOE Safety Analysis Process. It incorporates hazard identification, classification, and evaluation as well as accident analysis.

The hazard analysis:

- Determines the plant conditions, material, systems, processes, and characteristics that can produce undesirable consequences.
- Examines the complete spectrum of potential accidents that could expose members of the public, facility workers, and the environment to hazardous materials.

SAR and Accident Analysis

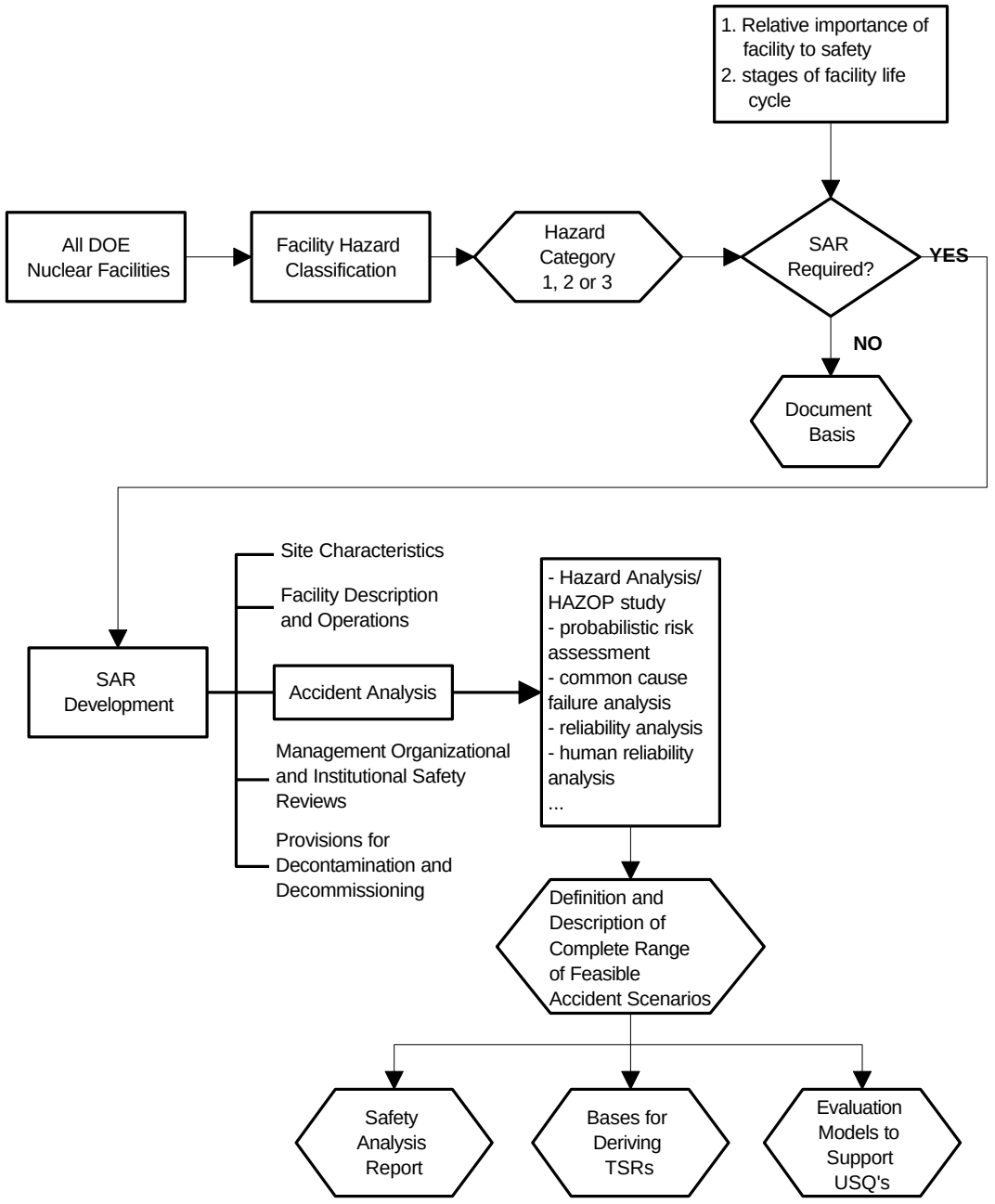
The accident analysis:

- Identifies any SSCs and TSRs that are needed to realize protection.
- Serves as explicit documentation on scenario progression and the analysis' assumptions for high-consequence accidents.

The range of accident scenarios included in the accident analysis should define the accident conditions envelope for the facility. The accident spectrum should range from frequently expected accidents to possible, but unlikely accidents.

Figure 7.3

DOE Safety Analysis Process



The accident analysis should demonstrate:

- adequate protection of health and safety for members of the public both on- and off-site
- adequate health and safety protection of workers onsite who are not involved in or responsible for the facility or its safety

- adequate protection of the environment from accidental contamination by the facility
- adequate protection of facility workers in order to support their reliable function of safety-related activities.

H. Identify the purpose and discuss the elements of Technical Safety Requirements.

Technical Safety Requirements (TSRs) are those conditions, operations, safe boundaries, and management or administrative controls necessary to:

- ensure safe operation of a nuclear facility
- reduce potential risk to the public and facility workers from
  - uncontrolled releases of hazardous materials
  - radiation exposure due to inadvertent criticality.

The TSR is important because it

- provides a focal point for important safety elements in the facility's highest level operational safety document
- provides a clear definition and actions for TSR violations
- formally defines the operational and programmatic safety elements of the safety envelope
- is a basic element of the Operational Readiness Review.

TSR Scope and Content

The scope and content of a TSR includes only the most critical nuclear safety areas. By restricting the TSR in this manner, it becomes operationally useful for controlling facility safety. The following paragraphs describe a TSR's contents.

1. Use and Application

   This section contains the definitions of terms, operating modes, frequency notations, and actions to be taken in the event that TSR operating limits or surveillance requirements are violated. This section contains the basic instructions for using and applying the safety restriction contained in the TSRs.

2. Safety Limits (SL)

   Safety Limits are limits on process variables associated with physical barriers which are necessary for the intended facility

function and which are required to guard against the uncontrolled release of radioactivity and other hazardous materials.

If any Safety Limit is exceeded at any reactor or nonreactor nuclear facility, action must begin immediately to place the facility in the most stable, safe condition attainable which could include total shutdown of either reactor or nonreactor nuclear facilities. The Safety Limits section describes the action to be taken when an SL is exceeded.

3. Operating Limits

   a. Limiting Control Settings (LCS)

      LCS' are settings on safety systems that control process variables in order to prevent exceeding Safety Limits. This subsection of the TSR contains the settings for automatic alarms and automatic or non-automatic protective actions initiation of those variables with significant safety functions. The specific settings are chosen to provide sufficient time to automatically or manually correct the condition prior to exceeding the Safety Limits.

   b. Limiting Conditions for Operation (LCO)

      LCOs are the lowest functional capability or performance level of safety-related structures, systems, component (SSCs) and their support systems required for normal, safe operation of the facility. This subsection of the TSR contains the limits on functional capability or performance level.

4. Surveillance Requirements

   These requirements relate to the test, calibration, or inspection of safety-related SSCs and their support systems to ensure that the necessary operability and quality is maintained. This section of the TSR contains the requirements necessary to maintain operation of the facility within the SLs, LCS', and LCOs.

5. Administrative Controls

   Administrative Controls are the provisions relating to organization, management, procedures, record-keeping, reviews, and audits necessary to ensure safe operation of the facility. This section of the TSR contains the requirements associated with Administrative Controls including those for reporting deviations from the Technical Safety Requirements

6. Appendices

a. Basis

This appendix provides summary statements on the reasons for the operating limits and associated surveillance requirements. The basis shows how the numeric value, the condition, or the surveillance fulfills the purpose derived from the safety documentation.

b. Design Features.

This appendix describes passive design features of the facility which, if altered or modified, would have a significant effect on safe operation.

I. Discuss the relationship between the Safety Analysis Report and the Technical Safety Requirements.

The TSRs commit the facility operators to maintain the safety basis as defined in the SAR.

SAR Background

The site-specific Safety Analysis Report and especially the safety analysis contained within the SAR are the source documents for developing the TSR's setpoints, limits, staffing requirements and other parameters.

The safety analysis considers:

- all credible accidents expected during facility lifetime
- all site-specific accidents
- any significant possible releases of radioactive and hazardous materials
- criticality scenarios.

A careful and thorough examination of the SAR's accident analysis yields:

- values necessary for defining the facility's operational limits to assure that facility operation does not occur outside the bounds assumed in the safety analysis
- parameters and operating conditions that should be limited in order to reduce, provide warning of, and mitigate the uncontrolled release of hazardous materials and to prevent inadvertent criticality
- technical and administrative conditions that must be met

- requirements for availability of safety equipment and systems.

Transition to TSR

The hazard and accident analyses within the SAR provide the most useful information for deriving TSRs. This information includes accident initial conditions, relevant parameters for safety SSCs, instrumentation, operator actions, assumed limits, and design features. Design features and administrative controls are derived from this information even though they are not addressed in other SAR chapters but are central to the TSRs.

The relationship between the SAR and the TSR can be further explained by considering the design and the operating envelopes.

SARs establish the Design Envelope	TSRs define the Operating Envelope
• commitments to design codes • facility and site parameters • accident analysis assumptions that determine performance criteria for safety SSCs • facility equipment drawings	• safety limits • limiting conditions for operation • limiting control setting • surveillance requirements • administrative controls

TSRs, SAR, and Margin of Safety

The last interface between the SAR and the TSRs is the Margin of Safety. TSRs

- present the minimal acceptable limits for operations under normal and specified failure conditions
- ensure that available equipment and initial conditions meet the assumptions found in the SAR's accident analysis
- extracts those aspects of the SAR that are required in order to assure the performance of SSCs and personnel as relied upon and defined in the SAR
- define the acceptance limits from which margins of safety may be determined
- explicitly defines the margin of safety – to the maximum extent practical.

J. Define who approves facility operations prior to achieving SAR upgrade approval.

Continued facility operations is approved by the Programmatic Secretarial Officer (PSO) by using the Preliminary SAR (PSAR) or pre-existing authorization (safety) basis.

K. Discuss those conditions that can lead to a determination of an inadequate safety analysis.

An inadequate safety analysis may occur when either a potential inadequacy in the currently accepted safety analysis as documented in the facility's SAR or a possible reduction in the margin of safety as defined by the TSRs is discovered.

When a potential inadequacy in any part of the authorization basis is discovered, the impact of this inadequacy may pose serious implications. It may be necessary to perform a safety analysis to determine conclusively whether a safety problem exists. DOE requires that an Unresolved Safety Question Determination (USQD) be completed immediately. The USQD provides a benchmark of the relative safety significance and places the facility into a safe condition.

DOE Order 5481.21, Unreviewed Safety Questions presents four situations that may involve an Unreviewed Safety Questions and a potential inadequate safety analysis:

- the probability of an occurrence or the consequences of an accident or malfunction of safety-related equipment can be increased
- the possibility for an accident or malfunction of a different type could be created
- a different type of accident or malfunction had been previously evaluated in a documented safety analysis
- any margin of safety, as defined in the TSRs, could be reduced.

When a potential inadequacy of a previous safety analyses is identified or a possible reduction in the margin of safety as defined in the TSRs is discovered, the technical manager shall:

- notify the PSO of the situation upon discovery of the information
- make an evaluation in accordance with paragraphs 10.a and 10.c of DOE Order 5480.21

- take action to place the facility in a safe condition until the safety evaluation is completed
- submit the complete safety evaluation prior to removing any operational restrictions initiated pursuant to paragraph 10.d.2.

L. Identify and describe the documentation that should be considered important to risk management.

Table 7.1

Risk Management Documentation

Document Number	Document Title
DOE Order 5480.19	Conduct of Operations Requirements
DOE Order 5480.20	Personnel Selection, Qualification, Training and Staffing Requirements at DOE Reactors and non-reactor Nuclear Facilities
DOE Order 5480.21	Unreviewed Safety Questions
DOE Order 5480.22	Technical Safety Requirements
DOE Order 5480.23	Safety Analysis Reports
DOE Order 5480.5	Safety of Nuclear Facilities
DOE Order 5480.6	Safety of Department of Energy-Owned Nuclear Reactors
DOE Order 232.1	Occurrence Reporting and Utilization of Operations Information
DOE Order 425.1	Startup and Restart of Nuclear Facilities
DOE Order 440.1	Worker Protection Management for DOE Federal and Contractor Employees
DOE Order 3790.1A	Federal Employees Occupational Safety and Health Program
DOE Order 460.1	Packaging and Transportation Safety
DOE Order 5480.3	Safety Requirements for the Packaging and Transportation of Hazardous Materials, Hazardous Substances and Hazardous Wastes
DOE Order 5610.1	Packaging and Transporting of Nuclear Explosives, Nuclear Components and Special Assemblies
DOE Order 452.1	Nuclear Explosive and Weapon Surety
DOE Order 452.2	Safety of Nuclear Explosive Operations
DOE Order 1324.5B	Records Disposition
DOE Order 430.1	Life-Cycle Asset Management

DOE Order 4700.1	Project Management System
DOE Order 5700.6C	Quality Assurance
DOE Order 6430.1A	General Design Criteria

M. Concerning industrial safety risks and hazards, describe typical methods for implementing the appropriate analysis and controls to ensure worker safety.

DOE's first safety responsibility must be the protection of the public and its workers. Those who work at DOE facilities accept some risk of exposure to radioactive and other hazardous materials due to the nature of the materials used and processed at the facilities. Nevertheless, it is incumbent upon DOE to assure that facilities operate in a manner that minimizes the risk to workers and limits exposure to hazardous materials to levels permitted by Federal or State regulations and relevant DOE Orders.

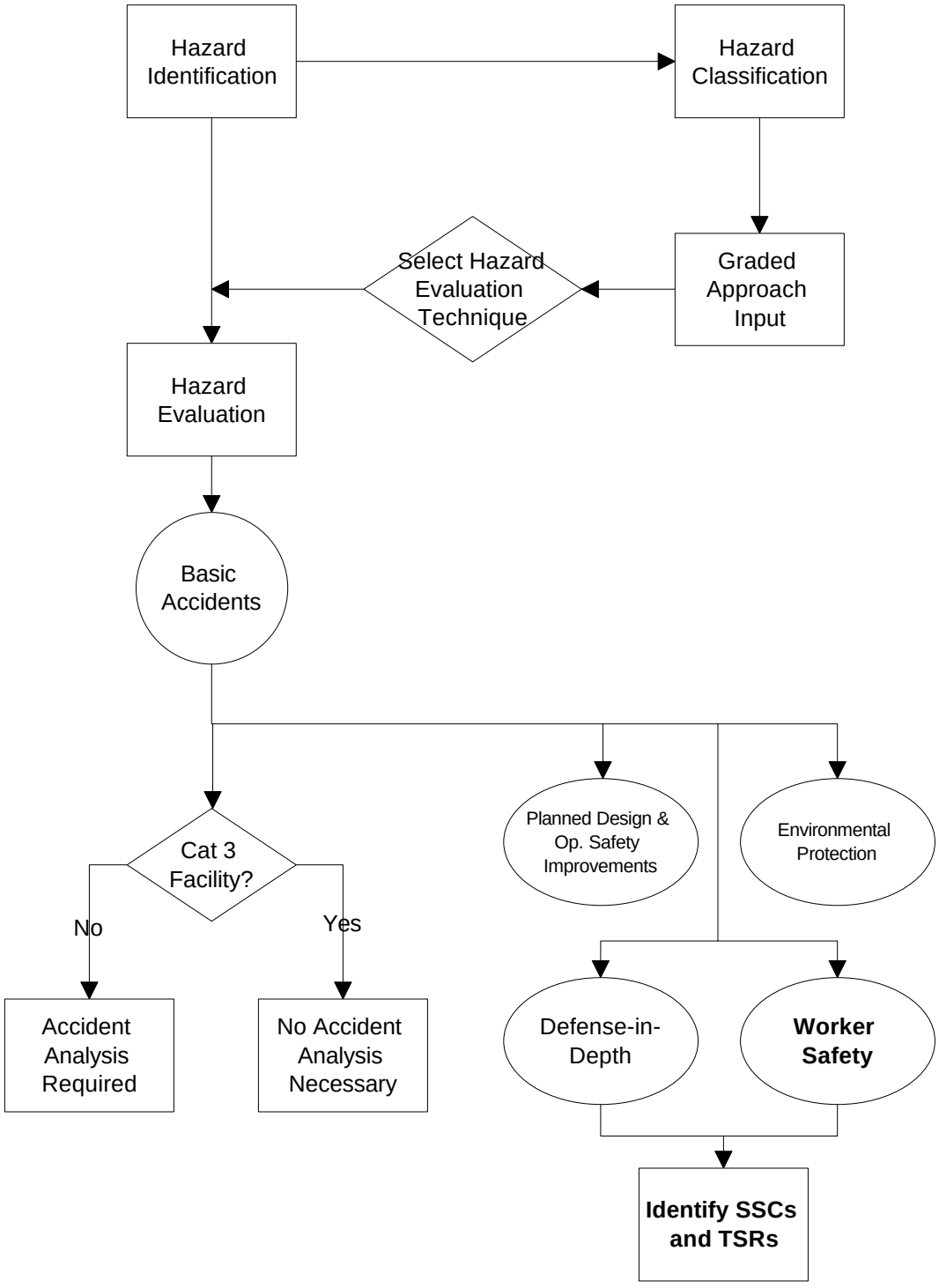
The SAR and Worker Safety

Traditionally, the safety, hazard and accident analyses focused on potential consequences to the public, but DOE Order 5480.23 emphasizes the worker as a population of concern. The methodology promoted in DOE-STD-3009-94, Non-reactor Nuclear Facility Safety Analysis Reports, requires answering the fundamental question of how worker safety is addressed in the SAR.

The methods for implementing analysis and controls to ensure worker safety at DOE nuclear facilities are the safety analysis and its component hazard evaluation and accident analysis. By using state-of-the-art hazard evaluation techniques and risk analysis, the managers of nuclear facilities can define and describe the complete range of accident scenarios. After identifying the basic accidents, management can implement barriers, controls, procedures, and systems to improve safety, implement defense-in-depth, and ensure facility worker safety in addition to public and environmental protection.

Figure 7.4 depicts the DOE Hazard Analysis Process. Please refer to the next page.

DOE Hazard Analysis Process **Figure 7.4**



Hazard Evaluation and Worker Safety

Hazard evaluation seeks to systematically identify facility hazards and accident potentials. This largely qualitative effort is the foundation for the entire safety analysis effort which addresses worker safety. The products of a hazard analysis are:

- a comprehensive evaluation of the complete accident spectrum
- hazards and release mechanisms
- preventative and mitigative features (SSCs and administrative)
- rough estimates of frequency and consequence
- potential design or operational improvement
- explanation of hazard analysis in terms of defense in depth and worker safety
- designation of safety SSCs and potential TSR issues
- identification of the limited set of accidents to formally document in the accident analysis.

The hazard analysis results should summarize the major features that protect workers from facility operations hazards and identify hardware that warrants a safety-significant SSC designation and/or TSR coverage based on the worker safety function. These SSCs are only identified for major threat potentials such as prompt fatalities or immediately life-threatening or permanently disabling injury; they do not focus on routine exposure related to potential latent effects.

SARs and Standard Industrial Hazards

Safety Analysis Reports specifically examine those hazards inherent in processes and related operations that can result in the uncontrolled release of hazardous materials or process-unique energy sources. Standard industrial hazards do not require SAR coverage. Standard industrial hazards such as burns from hot objects, electrocution, or falling objects are of concern only to the degree that they can be a contributor to a significant uncontrolled release of hazardous material or major energy sources.

OSHA recently published 10 CFR 1910.119, Process Safety Management of Highly Hazardous Chemical. Many topics covered in this federal regulation such as design codes and standards, process hazard analysis, human factors and training directly parallel the topics addressed by the SAR Order. The OSHA standard addresses

the issue of worker safety from process accidents by requiring the performance of hazards analysis for processes in conjunction with the implementation of basic safety programs which ensure that judgments made in hazard analyses are supported by actual operating conditions. These requirements effectively integrate programs and analyses into an overall safety management structure. This integration and the basic concepts of Process Safety Management (PSM) are accepted as appropriate for SARs. The OSHA standard effectively merges PSM principles with traditional nuclear SAR precepts.

TSRs and Worker Safety

Technical Safety Requirements, by requiring the facilities to operate within predetermined safety limits, not only protect the health and safety of facility workers but they also reduce risk to workers and facilities. TSRs are *not* based upon maintaining worker exposures below some acceptable level following an uncontrolled release of hazardous material or inadvertent criticality. The risk to workers is reduced through the reduction of the likelihood and potential impact of such events. This is accomplished by the development of safety requirements in the TSR for those systems, components, and equipment that

- are barriers preventing the uncontrolled release of radioactive and hazardous materials
- mitigate such releases
- prevent inadvertent criticality.

N. Discuss how proper risk and hazards management helps to ensure public and environmental protection.

The design of physical barriers to guard against radioactive and hazardous material releases protect the public and the environment. These barriers are designed to fulfill their operational function reliably by meeting all applicable criteria and standards. The defense-in-depth philosophy includes reliable design, provisions to safely terminate accidents, and provisions to mitigate the consequences of accidents. The health and safety protection functions are considered in the authorization basis and in the physical design as documented in safety analyses.

This protection philosophy pervades the accident analyses and DOE safety requirements. To understand and apply the defense-in-depth

philosophy, it is necessary to understand this perspective of maintaining the integrity of the physical barriers designed to contain hazardous and radioactive materials. This reflects the fact that accidents and malfunctions are analyzed in terms of their effect on physical barriers and that "consequences" are related to acceptance dose and hazardous-material release limits, depending on the event frequency.

The safety analyses for each nuclear facility establish the set of accident scenarios important to safe operation. The scenarios confirm the adequacy of the systems as well as equipment design and performance by identifying critical setpoints and operator actions and supporting the establishment of the Technical Safety Requirements. The final results of an accident analysis assumes that equipment functions as specified in the authorization basis under predetermined conditions.

The SAR considers analyses of potential accidents and demonstrates that, under the assumed accident conditions, the consequences of accidents challenging the integrity of the barriers will not exceed the criteria established by DOE. Changes that impact nuclear facility design and performance may affect the probability and consequences of accidents, create new accidents, and reduce margins of safety as defined in the bases of Technical Safety Requirements.

O. Describe the following types of documents and how they relate to nuclear risk management and hazard assessment:

- Safety Analysis Reports
- Technical Safety Requirements
- Inadequate Safety Analysis

Risk management and hazard assessment address the three basic questions of “What could go wrong?”, “How likely is it to go wrong?” and “What are the consequences?”.

Safety Analysis Reports

The SAR's safety analysis and its component hazard analysis and the accident analysis answer all three of these questions. The hazard analysis answers the first question while the accident scenarios carried forward into the accident analysis answer the second and third questions. The guidance document for DOE Order 5480.23 addresses the numerous risk assessment and hazard evaluation techniques that can be employed to determine which hazards exist at the facility.

Technical Safety Requirements

The TSRs are implemented to provide operating limits and surveillance requirements. The TSRs ensure the safe operation of the nuclear facility and provide risk management since they reduce the risk to workers, the public and the environment by reducing the likelihood and potential impact of hazardous material release or inadvertent criticality.

Inadequate Safety Analysis

The inadequate safety analysis which results in a Unreviewed Safety Question Determination is the mechanism for continually evaluating the safety basis and the margin of safety of a nuclear facility. It provides the guidance on action to take when an inadequate safety analysis is suspected or discovered. Inadequate safety analysis supports risk management and hazard assessment by forcing facility management to continuously review the safety basis and update Safety Analysis Reports and Technical Safety Requirements as new information or a changing facility status is discovered during safety evaluations.

P. Describe the risks associated with radioactive and hazardous wastes and the improper handling of that waste.

Identifying hazardous wastes or radioactive waste hazards and differentiating them from site risks is pivotal to effective hazardous and radioactive wastes management. For example, a chemical hazard such as toxicity, flammability, reactivity, or environmental mobility and persistence is an inherent characteristic of a chemical compound. The hazard is quantifiable, and it measures the inherent properties of a material to induce a particular adverse effect. Risk is a site- or incident-specific probability that harmful effects will occur. In order to calculate risk, the hazardous characteristics of a given

chemical are applied to the specific circumstances in which the chemical is found. In terms of chemical hazards, the risk or likelihood of death following a given exposure to a particular chemical is dependent upon the dose administered, the weight and health of the exposed individual, the route of exposure, and other factors.

Risk management is a measure of the potential for radioactive or hazardous wastes to escape from a source and communicate with sensitive receptors in the environment. The risk assessment interprets data about the source of contamination and articulates the effects the waste exerts on the environment. The goal of a risk assessment is to identify the level at which the effects of hazardous and radioactive waste become acceptable to current and future human and wildlife populations. From the information gleaned in the risk assessment, a remedial solution can be designed that will reduce unacceptable releases from the waste to the targeted risk level.

Two activities comprise hazardous and radioactive waste risk assessment:

1. Hazard characterization or compilation of site information:
   - identification of wastes
   - definitions of physiochemical and toxicological properties
   - determination of the physical and demographic properties of the site under investigation
2. Risk assessment: consideration of all the hazard characteristics and the potential adverse effect they represent.

A risk assessment can be approached in two tiers: a qualitative, descriptive assessment and a quantitative, measured or calculated assessment.

Qualitative Assessment

The analysis determines whether waste materials present at the site can be transported offsite. The analysis identifies the available pathways, determines whether any human or wildlife receptors can be reached by the wastes and identifies a set of transport and exposure scenarios. Figure 7-5 depicts the complete exposure pathway and its components. Each scenario encompasses a complete exposure pathway. The potential consequences of each scenario is the transmission of risk to receptors in the environs. The

probability, or risk, of any of these scenarios materializing is evaluated in the quantitative assessment.

Complete Exposure Pathway

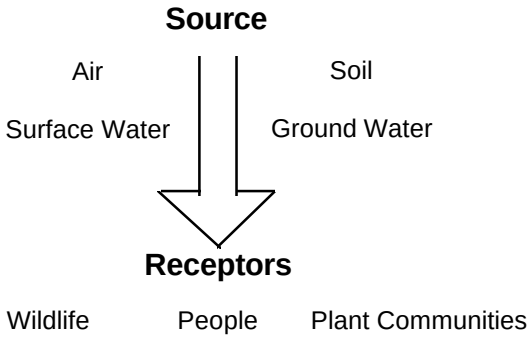


Figure 7.5

Table 7.2 lists the minimum data for a qualitative risk assessment and the site features reviewed in the assessment

Table 7.2

Qualitative Risk Assessment Data

Minimum Data Required	Site Features Reviewed
◆ climate of area ◆ geology of confining strata and formations ◆ seasonal levels of ground water ◆ horizontal and vertical extent of waste material and residues ◆ indication of type and depth of soil or other cover on site ◆ current and projected land use of site and environs ◆ human and wildlife population density in area ◆ use of ground water in area ◆ location of proximate surface water bodies ◆ nature of process that generated wastes ◆ volume and major hazardous constituents of wastes ◆ physiochemical properties of waste materials ◆ toxicity of waste materials	◆ geology of area, especially confining materials ◆ depth to bedrock ◆ physical dimensions ◆ depth to ground water ◆ seasonal ground water levels ◆ ground water flow velocity ◆ ground water use in the area ◆ average annual precipitation ◆ type and depth of soil cover ◆ extent of vegetative cover

Quantitative Assessment

The scenarios identified in the qualitative analysis are analyzed to define:

- the nature of any releases of wastes from the site
- the rates at which the wastes are transported from the site
- the specific populations of humans and wildlife exposed to the wastes
- the rates at which these compounds are entering the receptors' bodies.

The exposure rates are juxtaposed with known toxicological effects and compared with acceptable exposure rates in order to determine the urgency for remediation.

References and Suggested Reading

References and Suggested Reading

Department of Energy, DOE Order 232.1 Occurrence Reporting and Processing of Operations Information, DOE, 1995.

Department of Energy, DOE Order 425.1 Startup and Restart of Nuclear Facilities, DOE, 1995.

Department of Energy, DOE Order 5480.21 Unreviewed Safety Questions, DOE, 1991.

Department of Energy, DOE Order 5480.22 Technical Safety Requirements, DOE, 1992.

Department of Energy, DOE Order 5480.23 Nuclear Safety Analysis Reports, DOE, 1992.

Department of Energy, DOE Standard 1027-92 Hazard Categorization and Accident Analysis Techniques, DOE, 1992.

Department of Energy, DOE Standard 3006-93 Planning and Conduct of Operational Reviews, DOE, 1995.

Department of Energy (DP-31), DOE Standard 3009-94: Conceptual Basis and Hazard and Accident Analysis Process, Course Workbook, DOE, 1994.

Department of Energy - Albuquerque Operations Office, Safety Documentation: Authorization Basis for Facility Representatives, Course Workbook, DOE, 1996.

Haskin, F. E., Introduction to Hazard Evaluation and Risk Analysis, Course Notes, University of New Mexico,1994.

Hazardous Waste Site Remediation, O'Brien and Gere Engineers, Inc., Van Nostrand Reinhold, New York, NY, 1988.

Glossary of Terms

Accident	An unplanned event or sequence of events that results in undesirable consequences. An incident with specific safety consequences or impacts.
Accident Analysis	Those bounding analyses selected for inclusion in the SAR and refer only to design basis accidents.
Accident Sequence	The initiating events of an accident followed by combinations of successful and unsuccessful responses of structures, systems, or components.
Authorization Basis	Those aspects of the facility design basis and operational requirements relied upon by DOE to authorize operations. The Authorization Basis is described in documents such as the facility SAR and other safety analysis documentation.
Availability	A measure of the degree to which an item is in an operable and committable state at time *t*.
Causal Factor Chain	The cause-and-effect sequence in which a specific action creates a condition that contributes or results in an event. This creates new conditions that, in turn, result in another event.
Cause	A condition or an event that results in an effect which can be defined as anything that shapes or influences the outcome. A cause may be anything from noise in an instrument channel, a pipe break, an operator error, or a weakness or deficiency in management or administration.
Consequence	The direct, undesirable results of an accident sequence usually involving a fire, explosion, or release of hazardous or radioactive material. Consequence descriptions may be qualitative or quantitative estimates of the effects of an accident in terms of factors such as health impacts, economic loss, and environmental damage.
Corrective Action	The action identified to remedy the problem and prevent recurrence.
Cost-benefit analysis	The quantification of the decrease in risk versus the cost of proposed Structure, Systems and Components (SSCs) additions, modifications or eliminations.

Cut Set	A collection of basic events; if all the basic events occur, the top event is guaranteed to occur.
Design Basis	The set of requirements that bound the design of structures, systems and components within a facility.
Dominant Contributors	Accident sequences, starting with the highest risk in terms of quantified values that, when summed, encompass a majority (usually ≥ 90%) of the risk associated with the given facility or system being analyzed.
Event	A real-time occurrence such as a pipe break, a valve failure or a loss of power. An event is almost anything that could seriously impact the intended mission of DOE facilities.
Event Tree	Logic diagrams, at the system level of detail, which represent the combinations of system successes and failures that lead to unique sequences of events following each initiator. The tree depicts the various responses to the initiating event.
Fault Tree	Symbolic logic diagram that graphically show the cause-and-effect relationships of a system.
Hazard	A source of danger (i.e., material, energy source, or operation) with the potential to cause illness, injury, or death to personnel or damage to a facility or to the environment (without regard for the likelihood or credibility of accident scenarios or consequence mitigation).
Hazard Evaluation	The analysis of the significance of hazardous situations associated with a process or activity. Uses qualitative techniques to pinpoint weaknesses in the design and operation of facilities that could lead to accidents.
Hazard Identification	The pinpointing of material, system, process, and plant characteristics that can produce undesirable consequences through the occurrence of an accident.
Hazardous Materials	Those materials that are toxic, explosive, flammable, corrosive, or otherwise physically or biologically health threatening
Lessons-Learned	A "good work practice" or innovative approach that is identified and shared, or an adverse work practice or experience that is shared to avoid recurrence.

Margin of Safety	That margin built into the safety analyses of the facility as set forth in the authorization basis acceptance limits.
Minimal Cut Set	A combination of failures necessary and sufficient to cause the occurrence of the Top event in a fault tree.
Non-Reactor Nuclear Facility	A nuclear facility excluding reactors and accelerators.
Nuclear Facility	A facility that conducts activities or operations that involves radioactive and/or fissionable materials in such form and quantity that a nuclear hazard potentially exists to the employees or the general public. Included are reactors and accelerators.
Occurrence	.An event or a condition that adversely affects, or may adversely affect, DOE or contractor personnel, the public, property, the environment, or the DOE mission.
Probability	The likelihood of the occurrence of an event
Reliability	The probability that a product will perform its intended function satisfactorily for a pre-determined period of time in a given environment.
Risk	The quantitative or qualitative expression of possible loss that considers both the probability that an event will occur and the consequences of that event.
Risk Assessment	The process by which the results of a risk analysis are used to make decisions, either through relative ranking of risk reduction strategies or through comparison with risk targets.
Risk Management	The systematic application of management policies, procedures, and practices to the tasks of analyzing, assessing, and controlling risk in order to protect workers, the public, and the environment.
Root Cause	The cause that, if corrected, would prevent reoccurrence of this and similar events. The root cause not only applies to this event, but it has generic implications to a broad group of possible events. It is the most fundamental aspect of the cause that can logically be identified and corrected.

Safety	The elimination of hazards or the control of the hazards to levels of acceptable tolerance. A hazard is the source of energy and the physiological and behavioral factor which, when uncontrolled, leads to harmful occurrences.
Safety Analysis	A Safety Analysis is a process to systematically identify hazards of a DOE operation, analyze and evaluate potential accidents and their risks, and describe and analyze the adequacy of hazard control measures.
Safety Analysis Report (SAR)	SARs document the results of the safety analysis and describe the facility or activity, its design features, construction standards, operational modes and accident analysis.
Safety Basis	The information relating to the control of hazards at a nuclear facility upon which DOE depends for its conclusion that activities at the facility can be conducted safety.
Safety Envelope	The technically justified set of bounds on a facility's operations and design. The technical justification is derived from the accident analysis performed during the safety analysis while the safety envelope is substantiated and supported by the safety basis.
Sampling	The evaluation of a portion of a population (lot, batch, etc.) for the purpose of obtaining useful information about it. Inspection of a sample gives information about the quality of the pieces in a lot. Sampling also provides knowledge about the process which produced the lot.
Statistics	A scientific method used to collect, organize, summarize, present, and analyze data.
Technical Safety Requirements (TSR)	TSRs define the conditions, safe boundaries, and management or administrative controls necessary to ensure the safe operation of a nuclear facility.

Learning Activity-to-Competency Matrix

These are list of some of the learning activities available to address the competencies covered in this study guide.

Study Guide Section	Functional Area Competency	Activity Title	Activity Source
1.1 1.2 1.3 1.4 1.5 Statistics	EH 1.16, EC 1.6, CSE 1.4, ER 1.5	Certified Quality Engineer Primer, Self Study Course	Quality Council of Indiana
2.1 2.2 Event Tree and Fault Tree	NS 1.8	DOE Standard 3009-94: Conceptual Basis and Hazard and Accident Analysis Processes (24 Hrs)	DOE Defense Programs (DP-31)
3.1 3.2 Risk Assessment	CME 4.3, IC 4.4	Probabilistic Risk Assessment, Short Course	Massachusetts Institute of Technology
4.1 4.2 4.3 Problem Analysis	EH 4.3, EH 4.5, EC 4.15, CSE 4.4, CSE 4.5, ER 4,10, NS 4.5, CME 4.7, IC 4.7, IC 4.8, WM 4.9, ES 4.10, MS 4.8, CP 4.4, SS 4.10, SS 4.11, FM 4.5, FM 4.6, TM 3.1, FR 4.1	Principles of Accident Investigation	System Safety Development Center (Idaho)
5.1 Hazard Analysis	OS 1.2	DOE Standard 3009-94: Conceptual Basis and Hazard and Accident Analysis Processes (24 Hrs)	DOE Defense Programs (DP-31)

Study Guide Section	Functional Area Competency	Activity Title	Activity Source
6.1 6.2 Accident Analysis and Investigation	OS 1.4	Principles of Accident Investigation	System Safety Development Center (Idaho)
		DOE Standard 3009-94: Conceptual Basis and Hazard and Accident Analysis Processes (24 Hrs)	DOE Defense Programs (DP-31)
7.1 Nuclear Safety Analysis	WM 1.3, TM 1.5	DOE Standard 3009-94: Conceptual Basis and Hazard and Accident Analysis Processes & TSR Derivation (24 Hrs)	DOE Defense Programs (DP-45)
		SRSPO Self Study of the Safety Analysis Report	Savannah River Operations Office

Problem Analysis and Risk Assessment Study Guide
Cross Competency Listing

The following Matrix Shows where the Problem Analysis and Risk Assessment Study Guide addresses particular qualification standard competencies.

DOE Qualification Standards																Study Guide
EH Resident	Environ-mental Compliance	Civil/ Structural Engineering	Environ-mental Restoration	Nuclear Safety Systems	Construction Management & Engineering	Instrumen-tation and Control	Waste Management	Electrical Systems	Mechanical Systems	Chemical Processing	Safeguards and Security	Facility Mainten-ance Manage-ment	Technical Manager	Facilty Rep.	Occupa-tional Safety	
EH 1.16	EC 1.6	CSE 1.4	ER 1.5													PRA 1
				NS 1.8												PRA 2
					CME 4.3	IC 4.4										PRA 3
EH 4.3, 4.5	EC 4.15	CSE 4.4, 4.5	ER 4.10	NS 4.5	CME 4.7	IC 4.7, 4.8	WM 4.9	ES 4.10	MS 4.8	CP 4.4	SS 4.10, 4.11	FM 4.5, 4.6	TM 3.1	FR 4.1		PRA 4
															OS 1.2	PRA 5
															OS 1.4	PRA 6
							WM 1.3						TM 1.5			PRA 7

Basic Statistics
Cross Competency Listing

The following matrix shows where the Basic Statistics portion of the Study Guide addresses particular qualification standard competencies.

DOE Qualification Standards				Study Guide
Environment Safety and Health Resident	Environmental Compliance	Civil and Structural Engineering	Environmental Restoration	
ESH 1.16	**EC 1.6**	**CSE 1.4**	**ER 1.5**	**Section 1**
ESH 1.16.a	EC 1.6.a	CSE 1.4.a	ER 1.5.a	1-1
	EC 1.6.d	CSE 1.4.c	ER 1.5.c	1-1
	EC 1.6.e	CSE 1.4.d	ER 1.5.d	1-1
ESH 1.16.d	EC 1.6.f	CSE 1.4.e	ER 1.5.e	1-2
ESH 1.16.b	EC 1.6.b	CSE 1.4.b	ER 1.5.b	1-3
ESH 1.16.c	EC 1.6.c			1-3
ESH 1.16.f				1-4
ESH 1.16.e				1-5

PRA Terminology
Cross Competency Listing

The following matrix shows where the PRA Terminology portion of the Study Guide addresses particular qualification standard competencies.

DOE Qualification Standards Nuclear Safety Systems	Study Guide
NS 1.8	**Section 2**
NS 1.8.a	2-1
NS 1.8.b	2-2

Risk Assessment
Cross Competency Listing

The following matrix shows where the Risk Assessment portion of the Study Guide addresses particular qualification standard competencies.

DOE Qualification Standards		Study Guide
Construction Management and Engineering	**Instumentation and Control**	
CME 4.3	**IC 4.4**	**Section 3**
CME 4.3.a	IC 4.4.a	3-2A
CME 4.3.b	IC 4.4.b	3-2B
CME 4.3.c	IC 4.4.c	3-2C
CME 4.3.d	IC 4.4.d	3-2D
CME 4.3.e	IC 4.4.e	3-2E
CME 4.3.f	IC 4.4.f	3-2F
CME 4.3.g	IC 4.4.g	3-2G

Problem Analysis
Cross Competency Listing

The following matrix shows where the Problem Analysis portion of the Study Guide addresses particular qualification standard competencies.

DOE Qualification Standards															Study Guide
Environ-mental Restoration	**Chemical Processing**	**Waste Management**	**Civil/ Structural Engineering**	**Construction Management & Engineering**	**EH Resident**	**Electrical Systems**	**Mechanical Systems**	**Nuclear Safety Systems**	**Safeguards and Security**	**Environ-mental Compliance**	**Instrumen-tation and Control**	**Facility Mainten-ance Manage-ment**	**Technical Manager**	**Facilty Repre-sentative**	
ER 4.10	**CP 4.4**	**WM 4.9**	**CSE 4.4 CSE 4.5**	**CME 4.7**	**EH 4.5 EH 4.3**	**ES 4.10**	**MS 4.8**	**NS 4.5**	**SS 4.10 SS 4.11**	**EC 4.15**	**IC 4.7 IC 4.8**	**FM 4.5 FM 4.6**	**TM 3.1**	**FR 4.1**	**Section 4**
												FM 4.5.a	TM 3.1.c		4-1
													TM 3.1.d		4-1
													TM 3.1.a		4-2
ER 4.10.a	CP 4.4.a	WM 4.9.a	CSE 4.4.a		EH 4.3.a	ES 4.10.a	MS 4.8.a	NS 4.5.a	SS 4.10.a	EC 4.15.a		FM 4.5.e	TM 3.1.b	FR 4.1.a	4-3A, 4-3E
ER 4.10.b	CP 4.4.b	WM 4.9.b	CSE 4.4.b		EH 4.3.b	ES 4.10.b	MS 4.8.b		SS 4.10.b	EC 4.15.b		FM 4.5.f		FR 4.1.b	4-3B, 4-3D
	CP 4.4.c														
												FM 4.5.b			4-3C
		WM 4.9.f	CSE 4.4.f		EH 4.3.e			NS 4.5.e	SS 4.10.e		IC 4.7.c	FM 4.5.h		FR 4.1.e	4-3C
												FM 4.5.c			4-3E
														FR 4.1.e	4-3F
													TM 3.1.e		4-3G
ER 4.10.c	CP 4.4.d	WM 4.9.e	CSE 4.4.e CSE 4.5.a	CME 4.7.b	EH 4.5.a EH 4.3.f	ES 4.10.c	MS 4.8.c	NS 4.5.d	SS 4.11.a		IC 4.7.b IC 4.8.a	FM 4.6.a	TM 3.1.f	FR 4.1.c	4-3H
		WM 4.9.d	CSE 4.4.d	CME 4.7.a	EH 4.3.d			NS 4.5.c	SS 4.10.d		IC 4.7.a	FM 4.5.g		FR 4.1.d	4-3I
											IC 4.8.b			FR 4.1.f	4-3J
			CSE 4.5.b			ES 4.10.d	MS 4.8.d		SS 4.11.b						4-3K
			CSE 4.5.c	CME 4.7.e	EH 4.5.c	ES 4.10.e	MS 4.8.e		SS 4.11.c			FM 4.6.b			4-3K
			CSE 4.4.g												4-3L, 4-3C
			CSE 4.5.e												4-3M
			CSE 4.5.d	CME 4.7.d	EH 4.5.d	ES 4.10.f	MS 4.8.f		SS 4.11.d		IC 4.8.c	FM 4.6.c			2-2B
		WM 4.9.c	CSE 4.4.c		EH 4.5.b) EH 4.3.c			NS 4.5.b	SS 4.10.c	EC 4.15.c					6-2A

Hazard Analysis
Cross Competency Listing

The following matrix shows where the Hazard Analysis portion of the Study Guide addresses particular qualification standard competencies.

DOE Qualification Standards		Study Guide
Occupational Safety	**Nuclear Explosives Safety**	
OS 1.2		**Section 5**
OS 1.2.a		5-1A
OS 1.2.b	NES 1.9.a	5-1B
OS 1.2.c		5-1C
OS 1.2.d		5-1D
OS 1.2.e		5-1E
OS 1.2.f		5-1F

Accident Investigation
Cross Competency Listing

The following matrix shows where theAccident Investigation portion of the Study Guide addresses particular qualification standard competencies.

DOE Qualification Standard	Study Guide
Occupational Safety	
OS 1.4	**Section 6**
OS 1.4.c	6-1
OS 1.4.a	6-2
OS 1.4.b	6-2A
OS 1.4.d	6-2B
OS 1.4.f	6-2C
OS 1.4.g	6-2D
OS 1.4.e	Section 4-3E

Nuclear Safety Analysis
Cross Competency Listing

The following matrix shows where the Nuclear Safety Analysis portion of the Study Guide addresses particular qualification standard competencies.

DOE Qualification Standard		Study Guide
Waste Management	**Technical Manager**	
WM 1.3	**TM 1.5**	**Section 7**
WM 1.3.a	TM 1.5.a	7-1A
WM 1.3.b	TM 1.5.b	7-1B
WM 1.3.c	TM 1.5.c	7-1C
	TM 1.5.d	7-1D
	TM 1.5.e	7-1E
	TM 1.5.f	7-1F
	TM 1.5.g	7-1G
	TM 1.5.h	7-1H
WM 1.3.d	TM 1.5.i	7-1I
	TM 1.5.j	7-1J
WM 1.3.e	TM 1.5.k	7-1K
WM 1.3.f	TM 1.5.l	7-1K
	TM 1.5.m	7-1L
WM 1.3.h	TM 1.5.n	7-1M
WM 1.3.i	TM 1.5.o	7-1N
WM 1.3.g		7-1O
WM 1.3.j		7-1P